UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-014-1

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

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

Counsel for the North American Electric Reliability Corporation

May 23, 2014

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 2
II. NOTICES AND COMMUNICATIONS 7
III. BACKGROUND 7
A. Regulatory Framework 7
B. NERC Reliability Standards Development Procedure 8
C. The Physical Security Order 9
D. Procedural History of Proposed Reliability Standard CIP-014-1 13
IV. JUSTIFICATION FOR APPROVAL 15
A. Purpose and Overview of the Proposed Reliability Standard 15
B. Scope and Applicability of the Proposed Reliability Standard 17
C. Requirements in the Proposed Reliability Standard 29
D. Protection of Sensitive or Confidential Information 51
E. Enforceability of the Proposed Reliability Standards 53
V. EFFECTIVE DATE 54
VI. CONCLUSION 56

Exhibit A Proposed Reliability Standard
Exhibit B Implementation Plan
Exhibit C Order No. 672 Criteria
Exhibit D Consideration of Directives
Exhibit E Analysis of Violation Risk Factors and Violation Security Levels
Exhibit F Summary of Development History and Record of Development
Exhibit G Standard Drafting Team Roster

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

PETITION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION FOR APPROVAL OF PROPOSED RELIABILITY STANDARD CIP-014-1

Pursuant to Section 215(d)(1) of the Federal Power Act ("FPA"),[1] Section 39.5 of the regulations of the Federal Energy Regulatory Commission ("FERC" or "Commission"),[2] and the Commission's March 7, 2014 order issued in Docket No. RD14-6-000,[3] the North American Electric Reliability Corporation ("NERC")[4] hereby submits for Commission approval proposed Reliability Standard CIP-014-1 – Physical Security. NERC requests that the Commission approve the proposed Reliability Standard (Exhibit A) as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.[5] NERC also requests approval of (i) the associated Implementation Plan (Exhibit B), and (ii) the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibits A and E), as detailed in this Petition.

As required by Section 39.5(a) of the Commission's regulations,[6] this Petition presents the technical basis and purpose of proposed Reliability Standard CIP-014-1, a summary of its

---

1 16 U.S.C. § 824o (2006).

2 18 C.F.R. § 39.5 (2014).

3 *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014) (the "Physical Security Order").

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

5 Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

6 18 C.F.R. § 39.5(a) (2013).

development history (Exhibit F) and a demonstration that the proposed Reliability Standard meets the criteria identified by the Commission in Order No. 672[7] (Exhibit C). The NERC Board of Trustees adopted proposed Reliability Standard CIP-014-1 and the associated Implementation Plan on May 13, 2014.

I. EXECUTIVE SUMMARY

The Bulk-Power System is one of North America's most critical infrastructures and is uniquely critical as other infrastructure sectors depend on electric power. The reliability and security of the Bulk-Power System is fundamental to national security, economic development, and public health and safety. A major disruption in electric service due to extreme weather, equipment failure, a cybersecurity incident, or a physical attack could have far-reaching effects. Owners and operators of the Bulk-Power System must therefore institute measures to protect against and mitigate the impact of both conventional risks (e.g., extreme weather and equipment failures) and emerging security risks, such as physical attacks intended to damage or disable critical elements of the Bulk-Power System. As the Commission recognized in the Physical Security Order, "[p]hysical attacks to critical Bulk-Power System facilities can adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures."[8] The purpose of the proposed Reliability Standard is to enhance physical security measures for the most critical Bulk-Power System facilities and thereby lessen the overall vulnerability of the Bulk-Power System to physical attacks.[9]

---

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

[8] Physical Security Order at P 5.

[9] NERC's Reliability Standards already includes numerous Reliability Standards addressing both conventional risks and cybersecurity risks. Consistent with the Physical Security Order, the proposed Reliability Standard focuses on bolstering mandatory requirements addressing physical security risks.

The Commission's Physical Security Order provides a framework for a mandatory Reliability Standard that will represent a significant step forward in securing North America's most critical Bulk-Power System facilities. Proposed Reliability Standard CIP-014-1 requires Transmission Owners and Transmission Operators to protect those critical Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Consistent with the Physical Security Order, the proposed Reliability Standard requires Transmission Owners to take the following steps to address the risks that physical attacks pose to the reliable operation of the Bulk-Power System:

1) Perform a risk assessment of their systems to identify (i) their critical Transmission stations and Transmission substations, and (ii) the primary control centers that operationally (i.e., physically) control the identified Transmission stations and Transmission substations.

2) Evaluate the potential threats and vulnerabilities of a physical attack to the facilities identified in the risk assessment.

3) Develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of the identified critical facilities.

Further, the proposed Reliability Standard requires Transmission Operators that operate primary control centers that operationally control any of the Transmission stations or substations identified by the Transmission Owner to also:

1) evaluate the potential threats and vulnerabilities of a physical attack to such primary control centers; and

2) develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of such primary control centers.

Additionally, proposed Reliability Standard CIP-014-1 includes requirements for: (i) the protection of sensitive or confidential information from public disclosure; (ii) third party

verification of the identification of critical facilities as well as third party review of the evaluation of threats and vulnerabilities and the security plans; and (iii) the periodic reevaluation and revision of the identification of critical facilities, the evaluation of threats and vulnerabilities, and the security plans to help ensure their continued effectiveness.

The proposed Reliability Standard continues NERC's longstanding efforts to provide for the reliability and security of the Bulk-Power System. Even before the advent of mandatory Reliability Standards, NERC made grid security a priority, working with industry participants to address both physical and cyber security threats to critical assets. NERC currently addresses physical security through a combination of reliability tools, including security guidelines, training exercises, alerts, and mandatory standards. NERC's ongoing activities to addresses physical security issues include the following:

- NERC's Electricity Sector Information Sharing and Analysis Center ("ES-ISAC") monitors and analyzes Bulk-Power System events. The ES-ISAC then issues alerts through a secure portal to inform industry of physical and cyber threats, and to advise mitigation actions.
- NERC has security guidelines covering physical security response, best practices, and substation security.[10]
- Mandatory Reliability Standards that address certain aspects of physical security, including Reliability Standard EOP-004-2, which requires registered entities to report to NERC and law enforcement any physical damage to or destruction of a facility or threats to damage or destroy a facility, and Reliability Standard CIP-006-5, which includes requirements for the management of physical access to BES Cyber Systems.[11]
- NERC's Critical Infrastructure Protection Committee ("CIPC") was formed to advance the physical and cyber security of the critical electricity infrastructure of North America. Among other things, CIPC issues security guidelines and coordinates and communicates

[10] These guidelines address the following topics: (1) potential risks, (2) best practices that can help mitigate risks, (3) determination of organizational risks and practices appropriate to manage those risks, (4) identification of actions that industry should consider when responding to threat alerts received from the ES-ISAC and other organizations, (5) the scope of actions each organization may implement for its specific response plan, and (6) assessing and categorizing vulnerabilities and risks to critical facilities and functions.

[11] FERC approved Reliability Standard CIP-006-5 and it will becomes effective on April 1, 2016. CIP-006-5 replaces CIP-006-3c, which requires a physical security program for the protection of Critical Cyber Assets.

with organizations responsible for physical and cyber security in all electric industry segments, as well as other critical infrastructure sectors as appropriate.[12]

- NERC hosts grid security exercises, most recently GRIDEX II, to provide training and education opportunities for industry and government participants across North America.
- NERC hosts an annual Grid Security Conference ("GridSecCon") where experts discuss in detail a range of physical security issues.[13]
- NERC regularly participates in energy sector classified briefings both in the United States and Canada.
- NERC regularly works with industry and government partners on security matters through both formal and informal structures.[14]

This multi-pronged approach provides a framework for addressing the dynamic issues of physical and cyber security and helps to ensure a secure and reliable Bulk-Power System for North America. NERC's actions following a physical security incident at a California substation in April 2013 illustrate how NERC uses its multi-pronged approach to inform industry of security incidents and provide guidance on steps to mitigate and protect against future attacks.[15] Immediately after the incident, NERC's ES-ISAC issued an alert to industry to raise awareness of the seriousness and sophistication of the incident. Following this initial alert, NERC continued to work with the owner of the transmission substation to learn about the incident and communicate lessons learned to the industry. Additionally, NERC planned and participated in a 13-city outreach effort across the U.S. and Canada to raise awareness of the incident, inform industry of tactics and tools to

[12] The CIPC has a Physical Security Subcommittee that regularly discusses and analyzes physical security issues for education and awareness among the industry.

[13] NERC provides free physical security training in association with GridSecCon.

[14] For instance, NERC participates in the Electricity Sub-sector Coordinating Council, which provides a forum for communication between public and private sector partners in the Electricity Sub-sector

[15] The April 2013 incident did not result in a power outage. The owner of the substation worked diligently to maintain reliable operations and share lessons learned with government authorities and industry.

mitigate similar security risks, and provide a forum for industry participants to meet with state, local, and federal authorities to discuss physical security concerns in their regions.[16]

Although physical threats to the Bulk-Power System are not new, they are evolving and, as the incident in California illustrates, continue to demand NERC's and the industry's attention. The proposed Reliability Standard will enhance NERC's foundational physical security efforts and help ensure that owners and operators of the Bulk-Power System take the necessary steps to protect the Bulk-Power System from physical attacks. Additionally, as discussed further below, in approving proposed Reliability Standard CIP-014-1, the NERC Board of Trustees instructed NERC management to monitor and assess the implementation of the proposed Reliability Standard and provide regular updates to the Board of Trustees to measure the effectiveness of industry's implementation of the proposed Reliability Standard.

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

[16] This outreach effort involved, among others, NERC's ES-ISAC, the Department of Energy, FERC, the Department of Homeland Security, and the Federal Bureau of Investigation.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[17]

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

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

III. BACKGROUND

A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[18] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Nation's Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1)[19] of the FPA states that all users, owners, and operators of the Bulk-Power System in the United States will be subject to Commission-approved Reliability Standards. Section 215(d)(5)[20] of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability

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

[18] 16 U.S.C. § 824o (2006).

[19] *Id.* § 824(b)(1).

[20] *Id.* § 824o(d)(5).

Standard. Section 39.5(a)[21] of the Commission's regulations requires the ERO to file for Commission approval each Reliability Standard that the ERO proposes should become mandatory and enforceable in the United States, and each modification to a Reliability Standard that the ERO proposes to make effective.

The Commission has the regulatory responsibility to approve Reliability Standards that protect the reliability of the Bulk-Power System and to ensure that such Reliability Standards are just, reasonable, not unduly discriminatory or preferential, and in the public interest. Pursuant to Section 215(d)(2) of the FPA[22] and Section 39.5(c)[23] of the Commission's regulations, the Commission will give due weight to the technical expertise of the ERO with respect to the content of a Reliability Standard.

B. NERC Reliability Standards Development Procedure

The proposed Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[24] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards Development) of its Rules of Procedure and the NERC Standard Processes Manual.[25] In its ERO Certification Order, the Commission found that NERC's proposed rules provide for reasonable notice and opportunity for public comment, due process, openness, and a balance of interests in developing Reliability Standards and thus satisfies certain of the criteria for approving Reliability

---

21 18 C.F.R. § 39.5(a) (2012).

22 16 U.S.C. § 824o(d)(2).

23 18 C.F.R. § 39.5(c)(1).

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

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

Standards. The development process is open to any person or entity with a legitimate interest in the reliability of the Bulk-Power System. NERC considers the comments of all stakeholders, and a vote of stakeholders and the NERC Board of Trustees is required to approve a Reliability Standard before NERC submits the Reliability Standard to the Commission for approval.

C. The Physical Security Order

On March 7, 2014, the Commission issued the Physical Security Order directing NERC to submit for approval, within 90 days of the order, one or more Reliability Standards to address physical security risks and vulnerabilities of critical facilities on the Bulk-Power System. Although the Commission recognized that NERC and the industry have "engaged in longstanding efforts to address the physical security of its critical facilities,"[26] the Commission maintained that "to carry out section 215 of the FPA and to provide for the reliable operation of the Bulk-Power System," it was necessary to develop a mandatory Reliability Standard to "specifically require entities to take steps to reasonably protect against physical security attacks on the Bulk-Power System."[27]

The Commission stated that the Reliability Standard(s) should require owners and operators of the Bulk-Power System to take a least three steps:

- First, they should be required to "perform a risk assessment of their systems to identify their 'critical facilities.'"[28]
- Second, they should be required to "evaluate the potential threats and vulnerabilities to those identified critical facilities."[29]

---

[26] Physical Security Order at P 12.

[27] *Id*. at P 5.

[28] *Id*. at P 6.

[29] *Id*. at P 8.

- Third and finally, they should be required to "develop and implement a security plan designed to protect against attacks to their critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security."[30]

Additionally, the Commission stated that the proposed Reliability Standard(s) should also include: (1) procedures to ensure confidential treatment of sensitive or confidential information; (2) procedures for a third party to verify the list of identified facilities and allow the verifying entity, as well as the Commission, to add or remove facilities from the list of critical facilities; (3) procedures for a third party to review of the evaluation of threats and vulnerabilities and the security plan; and (4) a requirement that the identification of the critical facilities, the evaluation of the potential threats and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness.

The following is a brief discussion of each of the elements that the Commission stated should be included in any proposed Reliability Standard.

Identification of Critical Facilities: The Commission explained that the purpose of the risk assessment to identify critical facilities is to "ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System."[31] As such, the Commission explained, a "critical facility" for purposes of the Physical Security Order "is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk Power System."[32] The

---

30 Physical Security Order at P 9.

31 *Id*. at P 6.

32 *Id*. at P 6. The Commission recognized that "owners and operators may also take steps to protect facilities necessary to serve critical load on their systems, even if the inoperability or damage to those facilities would not result in instability, uncontrolled separation or cascading failures on the Bulk-Power System." *Id*. at n. 5. However, the Commission continued, the Reliability Standards should have a narrower purpose and apply only to

Commission explained that critical facilities will generally include critical substations and control centers.[33]

The Commission specified that "methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment," but did not require NERC to adopt a specific type of risk assessment, nor did the Commission require that a mandatory number of facilities be identified as critical facilities under the Reliability Standard(s).[34] The Commission stated, however, that it did not expect there to be a large number of critical facilities identified under the any proposed Reliability Standard:

> Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard.[35]

Evaluation of Threats and Vulnerabilities: The Commission recognized that "threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target."[36] Thus, the Commission stated, "the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated."[37] The Commission also stated that NERC should consider whether to

---

critical facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. *Id*.

33 Physical Security Order at n. 6.

34 *Id*. at P 6.

35 *Id*. at P 12.

36 *Id*. at P 8.

37 *Id*. at P 8.

require owners and operators to consult with entities with appropriate expertise as part of the evaluation process.[38]

Development and Implementation of a Security Plan: For the third step, the Commission recognized that there is not a "one size fits all" response to protect against physical security threats.[39] The Commission stated, however, that while the proposed Reliability Standard(s) need not "dictate specific steps an entity must take to protect against attacks on the identified facilities," it must "require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities."[40]

The Commission also stated that the Reliability Standard should allow applicable entities to consider elements of resiliency in carrying out these three steps, including system design, operation, and maintenance, and the sophistication of recovery plans and inventory management.[41]

Third Party Verification and Review: The Commission stated that the Reliability Standard should require that "the risk assessment used by an owner or operator to identify critical facilities [] be verified by an entity other than the owner or operator."[42] Additionally, the Physical Security Order provides that any proposed Reliability Standard "should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities."[43] Similarly, the Commission stated that under the Reliability Standard the "determination of threats and vulnerability and the security plan should also be

---

38 Physical Security Order at P 8.

39 *Id*. at P 2.

40 *Id*. at P 9.

41 *Id.* at P 7.

42 *Id*. at P 11.

43 *Id*. at P 11.

reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise."[44]

Reevaluation and Revision: Given the dynamic nature of the Bulk-Power System and physical security threats, the Physical Security Order provides that any proposed Reliability Standard "should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness."[45]

Confidentiality: Lastly, the Commission stated that the proposed Standard(s) should also include procedures that will ensure confidential treatment of sensitive or confidential information.[46] The Commission noted that compliance with a Reliability Standard including the three steps outlined in the order "could [lead to the development of] sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure."[47]

D. Procedural History of Proposed Reliability Standard CIP-014-1

As further described in Exhibit F hereto, following the issuance of the Physical Security Order, the NERC Standards Committee, working with NERC staff, initiated Project 2014-04 Physical Security to develop a proposed Reliability Standard to satisfy FERC's directive to submit one or more physical security Reliability Standards by June 5, 2014 (i.e., within 90 days of the Physical Security Order). To facilitate meeting the 90-day timeline, the NERC Standards

---

44 Physical Security Order at P 11.

45 *Id*. at P 11.

46 *Id*. at P 10.

47 *Id*. at P 10.

Committee approved waivers to the Standard Processes Manual to shorten the comment and ballot periods for the Standards Authorization Request ("SAR") and draft Reliability Standard.[48] In accordance with a Standard Committee-approved waiver of the Standard Processes Manual, NERC posted the SAR for a seven-day informal comment period from March 21-28, 2014. A NERC-led industry Technical Conference on April 1, 2014 provided an opportunity for the standards drafting team, NERC, and industry participants to discuss issues related to applicability, identification of critical facilities, evaluation of threats and vulnerabilities, development and implementation of physical security plans, and a proposed implementation plan for the proposed Reliability Standard.

On April 10, 2014, following standard drafting team meetings, NERC posted the proposed Reliability Standard for an initial 15-day comment period and 5-day ballot in accordance with the Standard Committee-approved waiver.[49] The initial ballot received a quorum of 88.60% and an approval of 82.07%. After addressing industry comments on the initial draft of the proposed Reliability Standard, NERC posted the proposed Reliability Standard for a final ballot, which received a quorum of 95.53% and approval of 85.61%.

The NERC Board of Trustees adopted proposed Reliability Standard CIP-014-1 and the associated Implementation Plan on May 13, 2014. In approving the proposed Reliability Standard, the NERC Board of Trustees articulated its expectation that NERC management monitor and assess implementation of the proposed Reliability Standard on an ongoing basis, including:

- the number of assets identified as critical under the proposed Reliability Standard;

[48] The Standards Committee approved the waivers in accordance with Section 16 of the Standard Processes Manual.

[49] On April 9, 2014, the Standards Committee authorized the posting of the proposed Reliability Standard for comment and ballot.

- the defining characteristics of the assets identified as critical;
- the scope of security plans (i.e., the types of security and resiliency measures contemplated under the various security plans);
- the timeliness included in the security plans for implementing the security and resiliency measures; and
- industry's progress in implementing the proposed Reliability Standard.

As directed by the NERC Board of Trustees, NERC staff could use this information to provide regular updates to the NERC Board of Trustees, FERC staff, and other applicable regulatory authorities on industry's progress in securing critical Bulk-Power System facilities. NERC staff would monitor implementation in a manner that protects against the public disclosure of any sensitive or confidential information by, among other things, collecting and presenting aggregated information that cannot be attributed to any particular entity or transmission system.

IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, proposed Reliability Standard CIP-014-1 satisfies the Commission's criteria in Order No. 672 and is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The following section provides an explanation of: (1) the purpose of the proposed Reliability Standard; (2) the scope and applicability of the proposed Reliability Standard; (3) each of the requirements in the proposed Reliability Standard, including a discussion of how the requirements fulfil each element of the Physical Security Order and enhance Bulk-Power System security; (4) the protection of sensitive or confidential information under the proposed Reliability Standard; and (5) the enforceability of the proposed Reliability Standard.

A. Purpose and Overview of the Proposed Reliability Standard

The proposed Reliability Standard serves the vital reliability goal of enhancing physical security measures for the most critical Bulk-Power System facilities and lessening the overall

vulnerability of the Bulk-Power System to physical attacks. As the Commission noted, physical attacks on critical elements of the Bulk-Power System could have a significant impact on the reliable operation of the Bulk-Power System, potentially resulting in instability, uncontrolled separation, or Cascading.[50] Although the April 2013 attack on a California substation did not result in a power outage and reliability was maintained throughout the incident,[51] it emphasizes the evolving nature of physical security risks and the need to bolster physical security measures through a combination of NERC's reliability tools, including mandatory Reliability Standards, to provide for a secure and reliable Bulk-Power System for North America.

Proposed Reliability Standard CIP-014-1 will reinforce NERC's and the industry's longstanding efforts to protect the Bulk-Power System from physical attacks. Consistent with the Physical Security Order, the proposed Reliability Standard requires Transmission Owners and Transmission Operators to take steps to address threats and vulnerabilities to the physical security of those Bulk-Power System facilities that present the greatest risk to reliability if damaged or otherwise rendered inoperable. As explained further below, the proposed Reliability Standard contains six requirements designed to protect against and mitigate the impact of physical attacks on certain Transmission stations and Transmission substations, and their associated primary control centers, as follows:

- *Requirement R1* requires applicable Transmission Owners to perform risk assessments on a periodic basis to identify their Transmission stations and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must then identify the primary control center that operationally controls each of the identified Transmission stations or Transmission substations.

- *Requirement R2* provides that each applicable Transmission Owner shall have an unaffiliated third party with appropriate experience verify the risk assessment performed

[50] Physical Security Order at P 5.

[51] No customers lost service during the incident.

under Requirement R1. The Transmission Owner must either modify its identification of facilities consistent with the verifier's recommendation or document the technical basis for not doing so.

- *Requirement R3* requires the Transmission Owner to notify a Transmission Operator that operationally controls a primary control center identified under Requirement R1 of such identification. This requirement helps ensure that such a Transmission Operator has notice of the identification so that it may timely fulfill its resulting obligations under Requirements R4 and R5 to protect that primary control center.

- *Requirement R4* requires each applicable Transmission Owner and Transmission Operator to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of its respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1, as verified under Requirement R2.

- *Requirement R5* requires each Transmission Owner and Transmission Operator to develop and implement documented physical security plan that covers each of its respective Transmission stations, Transmission substations, and primary control centers identified in Requirement R1, as verified under Requirement R2.

- *Requirement R6* provides that each Transmission Owner and Transmission Operator subject to Requirements R4 and R5 have an unaffiliated third party with appropriate experience review its Requirement R4 evaluation and Requirement R5 security plan. The Transmission Owner and Transmission Operator must either modify its evaluation and security plan consistent with the recommendation of the reviewer or document its reasons for not doing so.

B. Scope and Applicability of the Proposed Reliability Standard

As outlined above, the objective of proposed Reliability Standard CIP-014-1 is to identify and protect those critical Transmission stations and Transmission substations, and their primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. This scope is consistent with the Commission's directive in the Physical Security Order that the mandatory Reliability Standard focus industry resources on protecting the highest priority facilities on the Bulk-Power System. As discussed above, while the Commission recognized that owners and operators of the Bulk-Power System may also take steps to protect other types of facilities (i.e., "facilities necessary to serve critical load"), the Commission directed NERC to develop one

or more mandatory Reliability Standards that apply to facilities that would have significant or widespread impact on the Bulk-Power System if damaged or rendered inoperable as a result of a physical attack, namely, those "facilities that…could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[52]

Provided this direction, NERC and the standard drafting team determined that the appropriate focus of the proposed Reliability Standard is Transmission stations and Transmission substations, which are uniquely essential elements of the Bulk-Power System. They make it possible for electricity to move long distances, connect generation to the grid, serve as critical links or hubs for intersecting power lines, and are vital to the delivery of power to major load centers. Because of this functionality, Transmission stations and Transmission substations are the types of facilities that could meet the criteria for critical facilities set forth in the Physical Security Order. Damage to or the inoperability of certain large Transmission stations or Transmission substations has the potential to result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

The use of the phrase "Transmission stations or Transmission substations" in the applicability section and the requirements of the proposed Reliability Standard clarifies that the Reliability Standard applies to both "Transmission stations" and "Transmission substations," as industry uses those terms. Although these terms are sometimes used interchangeably, some entities consider the term "Transmission substation" to refer specifically to a facility contained within a physical border (e.g., a fence or a wall) that contains one or more autotransformers. In contrast, some entities use the term "Transmission station" to refer specifically to a facility that

[52] Physical Security Order at P 6 and n. 5.

functions as a switching station or switchyard but does not contain autotransformers. The proposed Reliability Standard uses both "Transmission station" and "Transmission substation" to make clear that both types of facilities are subject to the proposed Reliability Standard.

Following its determination that Transmission stations or Transmission substations are the appropriate focus of the proposed Reliability Standard, the standard drafting team recognized that it was also necessary to identify and protect the primary control centers that operationally control any critical Transmission stations or Transmission substations. A primary control center is a control center that the Transmission Owner or Transmission Operator uses as the principal, permanently-manned site to operate a Bulk-Power System facility. A primary control center operationally controls a Transmission station or Transmission substation when the electronic actions from the control center can cause direct physical actions at the identified Transmission station or Transmission substation, such as opening a breaker. If a physical attack damages or otherwise renders such a primary control center inoperable, it could jeopardize the reliable operation of the critical Transmission station and Transmission substation in Real-time because it could remove or severely limit the ability to operate that critical facility remotely to respond to events on the system or otherwise ensure the reliable operation of a critical Bulk-Power System facility. Similarly, if perpetrators of a physical attack seize a primary control center that operationally controls a critical Transmission station or Transmission substation, the attackers could directly operate the critical Transmission station and Transmission substation to cause significant adverse reliability impacts.

Control centers that provide back-up capability and control centers that cannot operationally control a critical Transmission station or Transmission substation do not present similar direct risks to Real-time operations if they are the target of a physical attack. If a physical

attack damages or renders inoperable a backup control center for a critical Transmission station or Transmission substation, it would have no direct reliability impact in Real-time as the entity can continue operating the Transmission station or Transmission substation from its primary control center. Backup control centers are maintained in a dormant, stand-by state. A backup control center is a form of resiliency built into the system and is therefore intentionally redundant. So long as the proposed Reliability Standard requires the Transmission Owner or Transmission Operator to adequately protect its primary control center(s), it need not also require the Transmission Owner or Transmission Operator to protect its backup control center(s). Nothing in the proposed Reliability Standard, however, prohibits a Transmission Owner or Transmission Operator from considering whether to implement security measures at its backup control centers to strengthen the resiliency of its system and the ability to recover from a physical attack.

Similarly, the standard drafting team concluded that a physical attack at a control center of a Reliability Coordinator, for instance, that only has monitoring or oversight capabilities of a critical Transmission station or Transmission substation[53] would not have the direct reliability impact in Real-time contemplated in the Physical Security Order because operators at such control centers do not have the ability to physically operate critical Bulk-Power System facilities. Although certain monitoring and oversight capabilities might be lost as a result of a physical attack on such controls centers, the Transmission Owner or Transmission Operator that operationally controls the critical Transmission station or Transmission substation would be able to continue

[53] Certain Independent System Operators ("ISO") and Regional Transmission Organizations ("RTO"), for instance, operate control centers that monitor the transmission system within their footprint. These control centers, however, have no capability to physically operate those facilities. Rather, the ISO/RTO, in their role as Reliability Coordinator or Transmission Operator, only has the authority to coordinate or direct the action of the entity that actually physically operates the facility at local control centers.

operating its transmission system to prevent widespread instability, uncontrolled separation, or Cascading within an Interconnection.

Importantly, while the proposed Reliability Standard only covers primary control centers that operationally control a critical Transmission station or Transmission substation, the physical security protections required under Reliability Standard CIP-006-5 are applicable to primary and backup control centers of Reliability Coordinators, Balancing Authorities, Transmission Operators and Generation Operators irrespective of their ability to operationally control Bulk-Power System facilities. Reliability Standard CIP-006-5 requires entities to implement physical security measures designed to restrict physical access to locations containing High and Medium Impact BES Cyber Systems. Such locations include primary and backup control centers that perform the functional obligations of Reliability Coordinators, Balancing Authorities, Transmission Operators, and Generation Operators.[54] While the measures implemented under Reliability CIP-006-5 are primarily designed to protect against a cyber attack, these measures also help protect such control centers from physical attack. Additionally, NERC understands that Reliability Coordinators, Balancing Authorities, Transmission Operators, and Generation Operators typically include physical intrusion controls for their control centers, such as barriers and fences, card key access restrictions, and manned-security, and have done so for many years outside the scope of mandatory Reliability Standards. For the reasons stated above, however, the standard drafting team concluded that the scope of the proposed Reliability Standard should only provide additional physical security

[54] Specifically, Reliability Standard CIP-002-5.1 provides that BES Cyber System located at primary and backup control centers that perform the functional obligations of Reliability Coordinators, Balancing Authorities, Transmission Operators and Generation Operators are "High Impact" or "Medium Impact" BES Cyber Systems.

protections to those primary control centers that can physically operate critical Transmission stations and Transmission substations.[55]

The standard drafting team also considered whether the scope of the proposed Reliability Standard should include other types of facilities, such as generation facilities (e.g., a generation plant or a generator collector bus). The standard drafting team concluded that while the loss of a generation facility due to a physical attack may have local reliability effects, the loss of the facility is unlikely to have the widespread, uncontrollable impact that the Commission was concerned about in the Physical Security Order. A generation facility does not have the same critical functionality as certain Transmission stations and Transmission substations due to the limited size of generating plants, the availability of other generation capacity connected to the grid, and planned resilience of the transmission system to react to the loss of a generation facility. For example, as required by NERC's Transmission Planning (TPL) group of Reliability Standards, planning models must account for the loss of a generation facility, and entities must build resiliency into their systems to withstand an N-1 contingency (e.g., the loss of a generator or a generation switchyard). Accordingly, a physical attack that damages a generation facility is highly unlikely to destabilize the system, or cause uncontrolled separation or Cascading within an Interconnection. By limiting the scope of proposed Reliability Standard CIP-014-1 to Transmission stations,

[55] NERC recognizes that certain control centers categorized as "High Impact" or "Medium Impact" under Reliability Standard CIP-002-5.1 would not be subject to the proposed Reliability Standard. This reflects the different nature of cyber security risks and physical security risks at control centers. An asset that presents a heightened risk to the Bulk-Power System from a cyber security perspective may not present the same risk from a physical security perspective and vice versa. A primary cyber security concern for control centers is the corruption of data or information and the potential for operators to take action based on corrupted data or information. This concerns exists at control centers that operationally control Bulk-Power System facilities and those that do not. As such, there is no distinction in CIP-002-5.1 between these controls centers. As discussed above, however, such a distinction is appropriate in the physical security context. As such, the standard drafting team concluded that each type of control centers categorized as "High Impact" or "Medium Impact" under CIP-002-5.1 does not necessarily need the additional protections provided by the proposed Reliability Standard.

Transmission substations and their associated primary control centers, industry will be able to focus resources where it is most essential for maintaining reliable operations.

Furthermore, Transmission Owners must consider the loss of generation in determining which Transmission stations or Transmission substations are critical for purposes of the proposed Reliability Standard. Specifically, any determination of whether a Transmission station or Transmission substation is critical under the proposed Reliability Standard would account for the loss of generation facilities connected to that Transmission station or Transmission substation. As stated in the technical guidance attached to proposed Reliability Standard CIP-014-1, in performing its risk assessment to identify critical Transmission stations and Transmission substations, "[a]n entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection." By doing so, a Transmission Owner would account for the loss of any generation connected to that Transmission station or Transmission substation.

As also explained and illustrated via a one-line diagram in the technical guidance attached to the proposed Reliability Standard, a Transmission station or Transmission substation that interconnects generation on the high side of a Generator Step-up transformer is subject to the Requirement R1 risk assessment, provided that the Transmission station or Transmission substation meets the criteria listed in Applicability Section 4.1.1, discussed below. The Requirement R1 risk assessment would then take into account the impact of the loss of a Transmission station or Transmission substation on the high-side of a Generator Step-up transformer that serves as an interconnection point for one or multiple generation resources.

Importantly, nothing in the proposed Reliability Standard precludes an entity from taking steps to protect against and mitigate the impact of physical attacks to generation facilities and control centers outside the scope of the proposed Reliability Standard, or any other Bulk-Power System element that does not meet the criteria of the proposed Reliability Standard. Many Reliability Coordinators, Balancing Authorities, Transmission Operators, Generation Owners, and Generation Operators are already taking steps to protect the physical security of their Bulk-Power System facilities, such as control centers and large generation facilities. NERC will continue to use its various reliability tools (e.g., security guidelines, training exercises, reliability assessments, and alerts) to inform industry of security threats and vulnerabilities and to provide guidance on steps industry participants should take to improve the security of all of their facilities to provide for a secure and reliable Bulk-Power System. Further, as noted above, Reliability Standards EOP-004-2 and CIP-006-5 address certain aspects of physical security.

Given the standard drafting team's determination on the appropriate scope of facilities subject to the proposed Reliability Standard, the proposed Reliability Standard provides requirements applicable to Transmission Owners and Transmission Operators, which are the functional entities that own and/or physically operate Transmission stations, Transmission substations and associated primary controls centers. Applying the proposed Reliability Standard to every registered Transmission Owner, however, would be overly broad, requiring many Transmission Owners to perform a risk assessment under Requirement R1 even though their systems do not include any Transmission stations or Transmission substations that would meet the Commission's criteria for critical facilities specified in the Physical Security Order. As the Commission recognized, "the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System" and many owners and

operators of the Bulk-Power System will not have critical facilities under the Reliability Standard.[56] NERC and the standard drafting team thus sought to establish a bright-line applicability threshold that would be broad enough to capture all Transmission Owners that could potentially have "critical facilities" while excluding Transmission Owners who do not own such facilities.

To that end, Applicability Section 4.1.1 of the proposed Reliability Standard provides that the proposed Reliability Standard applies only to those Transmission Owners that own a Transmission station or Transmission substation that meets the description of Transmission Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4. The Transmission Facilities included in Applicability Section 4.1.1.1 through 4.1.1.4 match the "Medium Impact" Transmission Facilities listed in Attachment 1 of Reliability Standard CIP-002-5.1.[57] The standard drafting team determined that using the criteria for "Medium Impact" Transmission Facilities set forth in Reliability Standard CIP-002-5.1 is an appropriate applicability threshold as the Commission has acknowledged that it is as a technically sound basis for identifying Transmission Facilities, which, if compromised, would present an elevated risk to the Bulk-Power System.[58]

Applicability Section 4.1.1 establishes an overinclusive threshold for defining which Transmission Owners are subject to the proposed Reliability Standard and must perform a risk assessment in accordance with Requirement R1. NERC expects that a number of Transmission Owners required to perform risk assessments under Requirement R1 will not identify any

---

[56] Physical Security Order at P 12.

[57] Specifically, the "Medium Impact" facilities described in Sections 2.4, 2.5, 2.6, and 2.7 of Attachment 1 of CIP-002-5.1.

[58] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160, Order No. 791-A, 146 FERC ¶ 61,188 (2013). As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits.

Transmission stations or Transmission substations that, if damaged or rendered inoperable as a result of physical attack, pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. Nevertheless, NERC and the standard drafting team concluded that using the "Medium Impact" criteria was a prudent approach to balancing the need for a Reliability Standard that is broad enough to capture all critical Transmission stations and Transmission substations while narrowing the scope of the Reliability Standard so as not to unnecessarily include entities that do not own or operate such critical facilities. During the development of the proposed Reliability Standard, the standard drafting team considered several other options for bright-line criteria but could not technically justify any higher threshold that would ensure the necessary Transmission stations and Transmission substations would be subject to the proposed Reliability Standard. Further, entities are already identifying whether they have "Medium Impact" facilities for purposes of transitioning to compliance with Reliability Standard CIP-002-5.1. As such, using the "Medium Impact" criteria in the applicability section of the proposed Reliability Standard does not create an additional burden on entities and complements the efforts already underway to comply with the CIP Reliability Standards approved in Order No. 791.

Transmission Operators are also subject to the proposed Reliability Standard (Applicability Section 4.1.2) to ensure that where the Transmission Owner does not operate the primary control center that operationally controls an identified Transmission station or Transmission substation, the Transmission Operator of that control center takes the steps required to protect that control center from physical attack. As discussed below, however, a Transmission Operator only has performance obligations under the proposed Reliability Standard if an applicable Transmission Owner notifies the Transmission Operator under Requirement R3 that the Transmission Operator

operates a primary control center that operationally controls a Transmission station or Transmission substation identified according to Requirement R1 (and verified under Requirement R2).

Finally, the standard drafting team considered whether it was necessary to include functional entities such as Reliability Coordinators or Balancing Authorities that have wide-area view of the Bulk-Power System as applicable entities under the proposed Reliability Standard. Specifically, whether such entities should be obligated to participate in the identification of critical facilities or have any responsibilities with respect to preventing or responding to physical attacks. Ultimately, for the reasons discussed below, the standard drafting team determined that expanding the scope beyond Transmission Owners and Transmission Operators would not provide any additional security benefits.

First, the standard drafting team concluded that the framework established in the proposed Reliability Standard accounts for a wide-area view and makes it unnecessary to include additional functional entities for purposes of identifying critical facilities. As explained further below, Transmission Owners are obligated to study in their risk assessments all of the categories of Transmission Facilities listed in Applicability section 4.1.1, including:

> Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

Accordingly, Transmission Owners are required to analyze Transmission stations and Transmission substations previously identified by Reliability Coordinators, Planning Coordinators, or Transmission Planners as potentially having a critical impact on the Bulk-Power

System.[59] Further, as noted above, the Commission already has acknowledged that the types of facilities listed in the applicability section reflect the subset of Transmission facilities that present an elevated risk to the Bulk-Power System.

Second, as further explained below, Requirement R2 obligates Transmission Owners to select an unaffiliated third party to verify their Requirement R1 risk assessment to help ensure that the identification of critical facilities captured the appropriate facilities. Requirement R2, Part 2.1 requires the verifying entity to be either a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator, or an entity that has transmission planning or analysis experience. Through this verification process, Transmission Owners can work with a third party with a wide-area view of the Bulk-Power System to help identify critical facilities that would have widespread impacts if compromised as a result of a physical attack.

Lastly, the standard drafting team concluded that it was not necessary to extend the applicability of the proposed Reliability Standard to Reliability Coordinators or Balancing Authorities for purposes of imposing responsibilities on such entities with respect to preventing or responding to physical attacks. The standard drafting team determined that any security measures to protect against or mitigate the impact of physical attacks on a particular facility most appropriately fall on the owner or operator of that facility, not another functional entity. Reliability Coordinators and Balancing Authorities, however, continue to have an important role, outside of the proposed Reliability Standard, in helping the system respond to or recover from a physical attack. Other Reliability Standards set forth the duties of functional entities in responding to events on the Bulk-Power System. The Emergency Preparedness and Operations (EOP) group of

[59] Interconnection Reliability Operating Limit are defined in the NERC Glossary as "[a] System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading outages that adversely impact the reliability of the Bulk Electric System."

Reliability Standards, for instance, include requirements for, among other things, emergency operations planning and coordination between the Reliability Coordinators, Balancing Authorities and Transmission Operators.[60] Proposed Reliability Standard CIP-014-1 will complement these Reliability Standards.

C. Requirements in the Proposed Reliability Standard

The following is an explanation of each of the requirements in the proposed Reliability Standard, including a discussion of how each requirement satisfies the elements of the Physical Security Order and enhances the reliability and security of the Bulk-Power System.

Requirement R1 addresses the directive in the Physical Security Order that entities should be required to perform a risk assessment of their systems to identify their critical facilities.[61] It also satisfies the directive for the periodic reevaluation and revision of the identification of critical facilities.[62] Requirement R1 requires Transmission Owners to conduct periodic risk assessment to identify their critical Transmission stations and Transmission substations. Requirement R1 provides:

> **R1.** Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria

---

60 For example, EOP-001-2.1b, Requirements R2 requires each Balancing Authority and Transmission Operator to develop, maintain, and implement a set of plans (i) to mitigate operating emergencies for insufficient generating capacity, (ii) to mitigate operating emergencies on the transmission system, (iii) for load shedding, and (iv) to mitigate operating emergencies. Under EOP-001-2.1b, Requirement R6 each Balancing Authority and Transmission Operator is also required to coordinate its operating plans with other Balancing Authorities and Transmission Operators. Further, Reliability Standard EOP-005-2, Requirement R1 requires the Transmission Operator to have a Reliability Coordinator approve its system restoration plan. Requirement R13 of that standard requires the Transmission Operator to have written agreements or mutually agreed to procedures with Generator Operators with blackstart resources, including testing requirements for those resources. Reliability Standard EOP-006-2 requires the Reliability Coordinator to have a Reliability Coordinator Area restoration plan and to coordinate restoration plans with other Reliability Coordinators and review the restoration plans of Transmission Operators within its Reliability Coordinator Area. The Reliability Coordinator is also required to work with Transmission Operators s, Generation Operators and adjacent Reliability Coordinators to monitor restoration and provide assistance if necessary.

61 Physical Security Order at P 6.

62 *Id*. at P 11.

specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1 Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2 The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

The applicability section and Requirement R1 effectively establish a two-step process for identifying critical facilities under the proposed Reliability Standard. First, a Transmission Owner must determine whether it has any Transmission stations or Transmission substations that meet the criteria in Applicability Section 4.1.1. If it does not, the Transmission Owner is not an applicable entity and has no performance obligations under the proposed Reliability Standard. If it does own Transmission stations or Transmission substations described in the applicability section, the Transmission Owner must then assess, in accordance with Requirement R1, whether any of those Transmission stations or Transmission substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

Requirement R1 mandates that the risk assessment "consist of a transmission analysis or transmission analyses" to help ensure that the methods used to identify critical facilities are based on objective analysis, technical expertise, and experienced judgment, consistent with the Commission's directive. The proposed Reliability Standard, however, does not require that a Transmission Owner use a specific method to perform its analysis. Transmission Owners have the ability to use the method that best suits their needs and the characteristics of their system. For example, an entity may perform a power flow analysis, which, depending on the characteristics of its system, could include a stability analysis at a variety of load levels as well as steady state or short circuit analyses under various system conditions and configurations.[63] The standard drafting team concluded that mandating a specific method would not adequately consider regional, topological, and system circumstances. Regardless of the method used to perform the risk assessment, however, Transmission Owners must be able to demonstrate to the verifier under Requirement R2 and the ERO during its compliance monitoring activities that it used an appropriate method to meet its affirmative obligation to identify all critical Transmission stations and Transmission substations under Requirement R1.[64]

As set forth in the Implementation Plan for proposed Reliability Standard CIP-014-1, Transmission Owners must complete their initial risk assessments on or before the effective date of the proposed Reliability Standard. Consistent with the Commission's directive, Requirement R1 also requires the periodic reevaluation and revision of the identification of critical facilities to

---

[63] The guidance section of the proposed Reliability Standard provides entities guidance on ways to perform the transmission analysis to meet the requirements of the standard.

[64] If a Transmission Owner patently fails to develop a method reasonably designed to identify its critical facilities (e.g., the assumptions underlying the study are patently deficient), the ERO could find that the Transmission Owner is non-compliant with Requirement R1 and exercise its enforcement authority against that Transmission Owner, as appropriate. As discussed below, in cases where the Transmission Owner demonstrates that the verifying entity is qualified, unaffiliated with the Transmission Owner, and the scope of their verification is clear, auditors are encouraged to rely on the verifications.

help ensure that the risk assessments remain current with projected conditions and configurations of the Transmission Owner's system. As provided in Requirement R1, Part 1.1, however, the timing of subsequent risk assessments depends on whether the Transmission Owner has previously identified any critical facilities. Specifically, if a Transmission Owner identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, it must conduct its next risk assessment within 30 calendar months of its previous risk assessment. The standard drafting team concluded that a 30-month period was appropriate given the long lead times required for a Transmission Owner to change its system, whether through construction of new facilities or otherwise, in a manner that would result in additional Transmission stations or Transmission substations meeting the criteria of a critical facility for purposes of the proposed Reliability Standard. Additionally, the 30-month period aligns with the requirement to consider both existing Transmission stations and Transmission substations and those planned to be in service within 24 months.

For a Transmission Owner that did not identify any critical facilities in its previous risk assessment (as verified according to Requirement R2), Requirement R1 requires the Transmission Owner to conduct its next risk assessment within 60 calendar months of its previous risk assessment. The standard drafting team concluded that because such entities are unlikely to see material changes to their systems in the Near-Term Planning Horizon that would result in a new or existing Transmission station or substation becoming critical, a 60-month period for completing subsequent risk assessments was appropriate.

Following the identification of any critical Transmission stations and Transmission substations, Part 1.2 requires the Transmission Owner to identify the primary control center that operationally controls each identified Transmission station and Transmission substation. As noted above, it is important to protect such primary control centers from a physical attack to help ensure that they are not damaged, rendered inoperable or misoperated in a way that could cause significant adverse reliability impacts.

Requirement R2 addresses the Commission directive that the Reliability Standard should (i) require that an entity other than the owner or operator verify the risk assessment, and (ii) include a procedure for the verifying entity to add or remove facilities from an owner's or operator's list of critical facilities.[65] Requirement R2 provides:

> **R2.** Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.
>
> **2.1.** Each Transmission Owner shall select an unaffiliated verifying entity that is either:
>
> - A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
>
> - An entity that has transmission planning or analysis experience.
>
> **2.2.** The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.
>
> **2.3.** If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each

[65] Physical Security Order at P 11.

recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or

- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

The purpose of the verification requirement is to have a third party with requisite expertise provide an independent assessment of the Transmission Owner's identification of critical facilities. As noted above, physical attacks on certain Transmission stations and Transmission substations could have a significant adverse impact on the reliable operation of the Bulk-Power System. Requirement R2 therefore builds in a layer of independence to help ensure that the Transmission Owner identifies and protects all critical Transmission stations and Transmission substations on its system. The third-party verification will also help provide additional assurance, consistent with the Physical Security Order, that the "methodologies to determine these facilities [are] based on objective analysis, technical expertise, and experienced judgment."[66]

To meet the intent of this element of the Physical Security Order, Requirement R2 requires that the verifying entity meet certain criteria. First, the verifying entity must be an "unaffiliated third party." For purposes of this Reliability Standard, the term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission

[66] *See* Physical Security Order at P 6.

Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.[67]

Additionally, the verifying entity must be a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator, or another entity that has transmission planning or analysis experience. In all cases, but particularly if the Transmission Owner does not select a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator, the Transmission Owner must demonstrate that the selected verifier has the requisite expertise to perform the verification. The guidance section of the proposed Reliability Standard includes a discussion of characteristics that Transmission Owners should consider when selecting a verifying entity, including: (1) experience in power system studies and planning; (2) understanding of the NERC MOD standards, TPL standards, and facility ratings as they pertain to planning studies; and (3) familiarity with the Interconnection within which the Transmission Owner is located. In cases where the Transmission Owner shows that the verifying entity is qualified, unaffiliated with the Transmission Owner, and the scope of their verification is clear, auditors are encouraged to rely on the verifications. In cases where the verifying entity lacks the qualifications specified in Requirement R2, the verifier is not sufficiently independent, or where the scope of the verification is unclear, it is expected that auditors will apply increased audit testing of Requirements R1.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout the risk

[67] The prohibition on Transmission Owners using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility be involved in the risk assessment process and have an opportunity to provide input, rather than to simply have an after-the-fact verification. Accordingly, Requirement R2 allows entities to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Consistent with the Commission's directive, Requirement R2 includes a process for the verifying entity to recommend the addition or removal of facilities from a Transmission Owner's list of identified facilities. Part 2.2 specifies that the verification "may include recommendations for the addition or deletion of a Transmission station or Transmission substation." Part 2.3 then requires the Transmission Owner to address those recommendations in one of two ways. The Transmission Owner must either: (i) modify its identification under Requirement R1 consistent with the verifier's recommendation(s); or (ii) document the technical basis for not modifying the identification in accordance with the recommendation. Requiring documentation of the technical basis for not modifying the identification in accordance with the recommendation will help ensure that a Transmission Owner meaningfully considers the verifier's recommendations and follows those recommendations unless it can technically justify its reasons for not doing so. To comply with Part 2.3, the technical justification must be sound and based on acceptable approaches to conducting transmission analyses. During its compliance monitoring activities, the ERO will

review that documentation in assessing the Transmission Owner's compliance with the proposed Reliability Standard.

Because the Commission has existing authority to enforce NERC Reliability Standards, the proposed Reliability Standard does not also include a procedure for the Commission to add or remove a facility from a Transmission Owner's list of identified facilities.[68] As provided in Section 215(e)(3) of the FPA and Section 39.7(f) of the Commission's regulations, the Commission has the authority, on its own motion, to enforce NERC Reliability Standards. In exercising that authority, the Commission, like NERC and the Regional Entities, can effectively require Transmission Owners to add or remove facilities if its finds that the Transmission Owner did not comply with its duty under Requirement R1 to identify critical Transmission stations or Transmission substations. As stated above, a Transmission Owner must be able to demonstrate that its method for performing its risk assessment was technically sound and reasonably designed to identify its critical Transmission stations and Transmission substations. If, in the course of assessing an entity's compliance with the proposed Reliability Standard, NERC, a Regional Entity, or FERC finds that the entity's transmission analysis was patently deficient and that the Requirement R2 verification process did not cure those deficiencies, they could use their enforcement authority to compel Transmission Owners to re-perform the risk assessment using assumptions designed to identify the appropriate critical facilities.

Requirement R2 also addresses the timing of the verifications. As provided in Part 2.2, the Transmission Owner is responsible for ensuring that the verifier completes the verification within 90 calendar days of the completion of each Requirement R1 risk assessment. The Transmission Owner then has 60 calendar days to modify its identification consistent with any recommendations

[68] *See* Physical Security Order at 11.

or document the technical basis for not doing so. The standard drafting team concluded that such timeframes appropriately balance the need to accomplish these tasks quickly while providing sufficient time for the Transmission Owner to complete the verification.

Lastly, consistent with the Commission's directive to protect confidential or sensitive information from public disclosure,[69] Part 2.4 creates an affirmative obligation on the Transmission Owner to guard against the release of any sensitive or confidential information, such as the list or location of critical Transmission Stations and Substations, to the public. As the Commission stated, if this information is disclosed to the public, it could jeopardize the reliable operation of the Bulk-Power System. Part 2.4 requires Transmission Owners to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier or otherwise developed pursuant to this Reliability Standard from public disclosure. Below is an additional discussion of confidentiality issues under the proposed Reliability Standard.

Requirement R3 provides:

> **R3.** For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.
>
> **3.1.** If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment,

[69] Physical Security Order at 10.

notify the Transmission Operator that has operational control of the primary control center of the removal.

Requirement R3 requires the Transmission Owner to notify a Transmission Operator that operationally controls a primary control center identified under Requirement R1 (as verified under Requirement R2) of such identification. Part 3.1 requires a Transmission Owner to notify the Transmission Operator of any removals from identification. This requirement helps ensure that such Transmission Operators have notice as to whether they have any obligations under the proposed Reliability Standard to protect any of their control centers.

Requirement R4 addresses the Commission's directive to require owners and operators evaluate the potential threats and vulnerabilities to their critical facilities.[70] It also satisfies the directive for the periodic reevaluation and revision of the evaluation of critical facilities.[71] Requirement R4 provides:

> R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:
>
> **4.1.** Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);
>
> **4.2.** Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and
>
> **4.3.** Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

---

[70] Physical Security Order at P 8.

[71] *Id*. at P 11.

Although Requirement R4 does not mandate a specific, one-size-fits-all method for evaluating potential threats and vulnerabilities, it obligates applicable entities to consider elements that form the foundation of an effective evaluation of security threats and vulnerabilities. First, consistent with the Commission's acknowledgement that threats and vulnerabilities may vary from facility to facility, Part 4.1 requires that the Transmission Owner or Transmission Operator tailor their evaluations to the unique characteristics of the facility in question so as to consider factors such as the facility's location, size, function, existing protections, and attractiveness as a target. Second, entities must consider prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events (Part 4.2). Lastly, entities must consider intelligence or threat warnings (Part 4.3). Collectively, Parts 4.1-4.3 help to ensure that the Transmission Owner and Transmission Operator tailor their evaluations to "the types of attacks that can be realistically contemplated," as the Commission directed.[72] The guidance section of the proposed Reliability Standard provides a list of resources that entities may consult for information on conducting effective threat and vulnerability evaluations.

Consistent with the directive in the Physical Security Order that the Reliability Standard require periodic evaluations, Transmission Owners and Transmission Operators must conduct an evaluation following each Requirement R1 risk assessment. Although Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur, Requirement R5, requires that entities develop their security plan(s) within 120 calendar days following completion of the Requirement R2 verifications. Because the development of the Requirement R5 security plan(s) is dependent on the completion of the Requirement R4 evaluation, Transmission Owners

[72] Physical Security Order at P 8.

and Transmission Operators must simply complete the Requirement R4 evaluation in time to comply with the 120-day period for completing the Requirement R5 security plan(s).

Requirement R5 addresses the Commission's directive to require owners and operators to develop and implement a security plan designed to protect against physical attacks to their critical facilities based on the assessment of the potential threats and vulnerabilities to those facilities.[73] It also satisfies the directive for the periodic reevaluation and revision of the security plans.[74] Requirement R5 provides:

> **R5.** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:
>
> **5.1.** Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.
>
> **5.2.** Law enforcement contact and coordination information.
>
> **5.3.** A timeline for executing the physical security enhancements and modifications specified in the physical security plan.
>
> **5.4.** Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

Requirement R5 creates an affirmative obligation on Transmission Owners and Transmission Operators to develop and implement security plans to protect their critical

---

[73] Physical Security Order at P 9.

[74] *Id*. at P 11.

Transmission stations, Transmission substations, and primary control centers. Rather than dictate the specific steps entities must take to protect their critical facilities, however, Requirement R5 obligates entities to develop security plan(s) that include elements that will help ensure that the security plans will result in an adequate level of protection against the potential physical threats and vulnerabilities identified pursuant to Requirement R4. These elements are set forth in Parts 5.1-5.4, each of which is discussed below.

Part 5.1 requires entities to include in their security plan(s) "[re]siliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4." Security measures refer to those steps an entity takes to strengthen the physical security of the site, such as security guards, video cameras, fences, or ballistic protections. Based on the Requirement R4 evaluation, entities should consider the need to implement security measures applicable to the entire site (e.g., the construction of a fence or wall around an entire facility, or the hiring security guards to guard the entire facility) as well as security measures that target specific critical components at the site (e.g., ballistic protections for some or all transformers at a Transmission substation).

Resiliency measures refer to those steps an entity may take that, while not specifically targeted as hardening the physical security of the site, help to decrease the potential adverse impact of a physical attack at an identified critical facility. These measures could include modifications to system topology or the construction of a new Transmission station or Transmission substation that would lessen the criticality of the facility. Entities may choose to focus their resources on redesigning their systems to limit the number of critical facilities, which will ultimately make it more difficult for the perpetrators of a physical attack to cause significant harm to the Bulk-Power

System.[75] Additionally, resiliency measures include providing for access to spare or replacement equipment. Many components of Transmission stations, Transmission substations, and primary control centers are expensive and difficult to replace quickly. Having spare equipment available will enable entities to limit the length of outages caused by a physical attacks. Entities should not necessarily be limited to implementing conventional security measures but should also seek to build resiliency into their system to enhance their ability to mitigate the risk and impact of a physical attack. The flexibility provided in Part 5.1 is thus consistent with the Commission's directive to allow applicable entities to consider elements of resiliency in identifying and protecting their critical facilities.

Part 5.2 requires entities to include in their security plan(s) provisions for "law enforcement contact and coordination information." Such provisions may include, among other things, providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services. Working with law enforcement is essential to both preventing and responding to physical attacks.

Part 5.3 requires entities to include in their security plan(s) a "timeline for executing the physical security enhancements and modifications specified in their physical security plan." Entities must have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors, such as the lead times necessary to implement certain security or resiliency measures. Entities must design these timelines, however, to protect their critical facilities from the threats and vulnerabilities identified pursuant to Requirement R4. For measures that have long lead times,

[75] The implementation of certain resiliency measures, such as the construction of a new Transmission station or Transmission substation, could affect the results of an entity's next Requirement R1 risk assessment such that a facility previously identified as critical would no longer meet that criteria.

entities must consider whether interim protections are necessary to address the identified threats and vulnerabilities. As part of the third party review of the security plans required by Requirement R6, as well as any ERO compliance monitoring activity, entities must be able to justify their implementation timelines and demonstrate that they are implementing their security plan in a manner that will provide an adequate level of protection as soon as reasonably practicable.[76]

Lastly, Part 5.4 requires entities to include in their security plans "[p]rovisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s)." These provisions will help ensure that a Transmission Owner's and Transmission Operator's physical security protections evolve to meet a dynamic and changing risk environment. An entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Such sources include the ERO, ES-ISAC, and US and/or Canadian federal agencies. Transmission Owners and Transmission Operators should then use that information to reevaluate or consider changes in the security plan and the corresponding security measures of the security plan.

The approach to specify the fundamental attributes that an entity must include in its security plan(s), as opposed to specifying the steps the entity must take, is consistent with the directives in the Physical Security Order[77] and preferable from a security perspective. As noted, the threat environment is dynamic and continually evolving. As such, Reliability Standards addressing security issues must allow entities to adapt to changing threats and encourage entities to develop

---

[76] If, in the course of assessing an entity's compliance with the proposed Reliability Standard, NERC, a Regional Entity, or FERC finds that the timelines were patently deficient in their ability to adequately deter, detect, delay, assess, communicate, and respond to the identified physical threats and vulnerabilities, they could use their enforcement authority to compel the Transmission Owners or Transmission Operator to modify those timelines.

[77] Physical Security Order at PP 2, 9.

and implement new and innovative measures to deter, detect, delay, assess, communicate, and respond to emerging security threats. As the Commission noted, there is not a one-size-fits all approach to protecting against physical security threats.[78] A specific measure that would be effective at one facility may not be appropriate for a different facility. Listing specific steps in the proposed Reliability Standard could also potentially stunt the types of security measures that entities would ultimately implement. Entities must have the flexibility to develop security measures that are unique to the threats and vulnerabilities of their facilities.

As described above, however, the plan must include measures designed "to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4." Accordingly, as part of the third party review of the security plans required by Requirement R6, as well as any ERO compliance monitoring activity, entities must demonstrate that their security plans are designed to result in an adequate level of protection against the potential physical threats and vulnerabilities identified pursuant to Requirement R4.

As to timing, Requirement R5 obligates Transmission Owners and Transmission Operators to develop (or revise) their security plans within 120 calendar days of the date the Transmission Owner completes Requirement R2.[79] This 120-day period is for the development of the plan, not implementation of the measures included with the security plan(s). Requirement R5 specifically states that entities must execute their security plans according to the timelines specified therein. As noted above, to comply with Requirement R5 Transmission Owners and Transmission

---

[78] See Physical Security Order at P 2.

[79] Requirement R2 is complete when there is nothing left to do under the requirement. If the verifier does not make any recommendations, then the Transmission Owner completes Requirement R2 once the verifier completes its verification. If the verifier makes one or more recommendations, the Transmission Owner only completes Requirement R2 when it has modified its identification of critical facilities consistent with the recommendations or documented its reasons for not doing so.

Operators must establish timelines reasonably designed to address the identified security threats and vulnerabilities to the critical facility in a timely manner.

Finally, Requirement R6 addresses the Commission directive that the Reliability Standard require that an entity other than the owner or operator of the critical facility review the Requirement R4 evaluation of threats and vulnerabilities and the Requirement R5 security plan(s). Requirement R6 provides:

> **R6.** Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5.
>
> **6.1.** Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:
>
> - An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
> - An entity or organization approved by the ERO.
> - A governmental agency with physical security expertise.
> - An entity or organization with demonstrated law enforcement, government, or military physical security expertise.
>
> **6.2.** The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.
>
> **6.3.** If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator

shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or

- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

Similar to Requirement R2, the purpose of Requirement R6 is to have a third party with the appropriate expertise provide an independent review of a Transmission Owner's and Transmission Operator's Requirement R4 evaluation or Requirement R5 security plans(s). The third party review will provide an additional layer of expertise and assurance that the Transmission Owner and Transmission Operator (1) properly evaluated potential threats and vulnerabilities, and (2) developed a security plan that results in an adequate level of protection against the potential physical threats and vulnerabilities it faces at the identified facilities.[80]

To meet the intent of this element of the Physical Security Order, Requirement R6 requires that the reviewing entity meet certain criteria. First, the reviewing entity must be an "unaffiliated third party." As in Requirement R2, the term "unaffiliated" means that the selected entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner or Transmission

[80] The third party review thus addresses the Commission directive that NERC should consider whether to require owners and operators to consult with entities with appropriate expertise as part of the evaluation process. *See* Physical Security Order at P 8.

Operator). The reviewing entity also cannot be a division of the Transmission Owner or Transmission Operator that operates as a functional unit.[81]

Additionally, Requirement R6 states that Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer that meets one of the following criteria: (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional ("CPP") or Physical Security Professional ("PSP") certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise;[82] and (4) an entity or organization with demonstrated law enforcement, government, or military physical security expertise. NERC and the standard drafting team determined that unaffiliated entities or organizations that meet these qualifications will have the expertise necessary to provide an effective and independent review. Applicable Transmission Owners and Transmission Operators have the flexibility to have one reviewer review both the Requirement R4 evaluation and the Requirement R5 security plan or have separate reviewers for each step.

Under either scenario, the Transmission Owner and Transmission Operator must show that the selected entity has the appropriate expertise to conduct the review. As noted for Requirement R2, in cases where the Transmission Owner or Transmission Operator shows that the reviewing entity is qualified, sufficiently independent, and the scope of their review is clear, auditors are encouraged to rely on the reviews. In cases where the reviewing entity lacks the qualifications

---

[81] The prohibition on Transmission Owners using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

[82] CPP and PSP certifications are widely-recognized in the physical security industry to demonstrate expertise in the physical security domain.

specified in Requirement R6, the reviewer is not sufficiently independent, or where the scope of the review is unclear, it is expected that auditors will apply increased audit testing of Requirements R4 and R5.

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision provides applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. In other words, a Transmission Owner or Transmission Operator could collaborate with its unaffiliated third party reviewer to perform the Requirement R4 evaluation or develop the Requirement R5 security plan. This collaboration may allow entities to create efficiencies in their processes for complying with the proposed Reliability Standard. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility be involved with and provide input on the Requirement R4 evaluation and the development of the Requirement R5 security plans, rather than simply have an after-the-fact review. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Requirement R6, Part 6.2 provides that applicable Transmission Owners and Transmission Operators are responsible for ensuring that the reviewer(s) complete the review within 90 calendar days of the completion of the development of the security plan under Requirement R5. Part 6.2 also specifies that the review may "include recommended changes to the evaluation performed

under Requirement R4 or the security plan(s) developed under Requirement R5." Part 6.3 then specifies that the Transmission Owner or Transmission Operator must address those recommendations, within 60 calendar days, in one of two ways. The Transmission Owner or Transmission Operator must either: (i) modify its evaluation or security plan consistent with the reviewer's recommendation(s); or (ii) document the reason for not modifying the evaluation or security plan in accordance with the recommendation. Requiring documentation of these reasons will help ensure that the Transmission Owner or Transmission Operator properly considers the reviewer's recommendations and follows those recommendations unless it can justify not doing so. The ERO or the Commission can then review that documentation when evaluating the entity's compliance with the proposed Reliability Standard. Although Part 6.3 allows the Transmission Owner or Transmission Operator to consider a variety of factors for not following the reviewer's recommendations, to satisfy Part 6.3, the Transmission Owner or Transmission Operator must provide a reasonable justification for not doing so.

Lastly, consistent with the Commission's directive to protect confidential or sensitive information from public disclosure,[83] Part 6.4 creates an affirmative obligation on the Transmission Owner and Transmission Operator to guard against the release of any sensitive or confidential information, such as site vulnerabilities or the security protection established for a particular site. Release of such information could provide a roadmap to those individuals or groups intent on physically attacking critical Bulk-Power System facilities. As the Commission stated, if this information is disclosed to the public, it could jeopardize the reliable operation of the Bulk-Power System.[84] Part 6.4 thus requires Transmission Owners to implement procedures, such as

---

83 Physical Security Order at 10.

84 *Id.*

the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and or otherwise developed pursuant to this Reliability Standard from public disclosure. Below is an additional discussion of confidentiality issues under the proposed Reliability Standard.

D. Protection of Sensitive or Confidential Information

As discussed above, the Commission sought to ensure that any sensitive or confidential information that entities develop in the course of complying with the proposed Reliability Standard remains confidential to decrease the possibility that such information could become available to individuals or groups that may use such information to perpetrate physical attacks on the Bulk-Power System.[85] To that end, the proposed Reliability Standard affirmatively obligates entities to protect their sensitive and confidential information from public disclosure (Requirement R2, Part 2.4 and Requirement R6, Part 6.4). Procedures for protecting confidential information may include, among other things, the following elements: (1) the control and retention of information at the applicable entity's facility for third party verifiers/reviewers; (2) restricting information to only those employees that need to know such information for purposes of carrying out their job functions; (3) marking all relevant documents as confidential; (4) securely storing and destroying information, both physical and electronically; and (5) requiring senior manager sign-off prior to releasing any sensitive or confidential information to an outside entity.

Additionally, the compliance monitoring section of the proposed Reliability Standard provides that all evidence for demonstrating compliance with this standard will be retained at the Transmission Owner's and Transmission Operator's facilities.[86] Requiring that evidence remain

---

[85] *Id.*

[86] Specifically, Compliance Monitoring Section 1.4 provides:

on site will reduce the possibility of releasing sensitive or confidential information to individuals who should not have access to such information. NERC and the Regional Entities will develop policies to ensure that sensitive or confidential information reviewed during compliance monitoring activities will remain on site and confidential.

During the standard development process, certain registered entities raised issues as to the relationship between the confidentiality provisions of the proposed Reliability Standard and public disclosure laws, such as the U.S. Freedom of Information Act, and similar state, provincial, or local laws. Registered entities were concerned that public disclosure laws would require them to publicly disclose certain sensitive or confidential information, thereby jeopardizing the reliability of the Bulk-Power System. NERC notes that the confidentiality provisions in proposed Reliability Standard CIP-014-1 may provide registered entities subject to public disclosure laws the authority to limit public disclosure of sensitive or confidential information developed pursuant to the proposed Reliability Standard. NERC understands that many public disclosure laws in various jurisdictions in the United States and Canada include provisions that exempt from public disclosure information that entities must keep confidential pursuant to another federal, state, provincial, or local law.[87] Such exemptions may apply to the sensitive or confidential information developed in the course of complying with the Reliability Standard given the affirmative obligation in the proposed Reliability Standard (Parts 2.4 and 6.4) that applicable entities protect such information from public disclosure. Additionally, certain public disclosure laws already exempt from disclosure certain confidential information specifically related to critical infrastructures, such as

> Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

[87] *See*, *e.g.*, Colorado Open Records Act, C.R.S. § 24-72-204; Washington Public Records Act, Wash. Rev. Code § 42.56.070.

energy, water, or telecommunications infrastructure,[88] or information that is vital to governmental interests.[89] Such provisions may exempt some, if not all, of the sensitive or confidential information developed under the standard from disclosure.

Nevertheless, NERC understands that public disclosure laws are different across the various jurisdictions in North America and there may be some laws that do not have existing provisions to exempt from public disclosure the sensitive or confidential information developed under the proposed Reliability Standard. The purpose of NERC Reliability Standards is to establish and impose mandatory requirements that owners, operators and users of the Bulk-Power System must follow to help protect the reliability of the Bulk-Power System. NERC Reliability Standards do not stipulate whether certain information is exempt from public disclosure laws. The applicability of such laws to the information developed under proposed Reliability Standard CIP-014-1 may be addressed in other forums at the federal, state, provincial, or local levels. NERC understands that certain registered entities may ask the Commission for a statement indicating that the proposed Reliability Standard will govern any contrary state or local public disclosure law. Such a statement could help to clarify the applicability of public disclosure laws and further the intent of the Physical Security Order to protect sensitive or confidential information.

E. Enforceability of the Proposed Reliability Standards

The proposed Reliability Standard includes VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standard. The VRFs and VSLs for the proposed Reliability Standard comport with NERC and

---

[88] *See, e.g.*, Arizona Public Records Act, A.R.S. §39-126 (stating "[n]othing in this chapter requires the disclosure of a risk assessment that is performed by or on behalf of a federal agency to evaluate critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack.")

[89] *See, e.g.*, Wash. Rev. Code § 42.56.210.

Commission guidelines related to their assignment. Exhibit E provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

The proposed Reliability Standard also includes measures that support each requirement by clearly identifying what is required and how the ERO will enforce the requirement. These measures help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.[90]

V. EFFECTIVE DATE

In the Physical Security Order, the Commission stated that "NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements."[91] The Commission also specified that the implementation plan should include timeframes for completion of the risk assessment, threat and vulnerability evaluations, and development and implementation of the security plan.

Consistent with the Commission's directive, NERC respectfully requests that the Commission approve the proposed Reliability Standard to become effective on the first day of the first calendar quarter that is six months after Commission approval. The Implementation Plan for proposed Reliability Standard CIP-014-1, attached hereto as Exhibit B, provides a timeline for initial performance under the proposed Reliability Standard following the proposed effective date.

---

[90] Order No. 672 at P 327 ("There should be a clear criterion or measure of whether an entity is in compliance with a proposed Reliability Standard. It should contain or be accompanied by an objective measure of compliance so that it can be enforced and so that enforcement can be applied in a consistent and non-preferential manner.").

[91] Physical Security Order at P 12.

As described in the Implementation Plan, applicable Transmission Owners must conduct their initial Requirement R1 risk assessment on or before the effective date of the proposed Reliability Standard. Transmission Owners and Transmission Operators must then complete initial performance of Requirements R2 through R6, as applicable, according to the timelines specified in those requirements, as follows:

- *Requirement R2* - The Transmission Owner must (i) complete the third party verification of the risk assessment (Parts 2.1, 2.2, and 2.4) within 90 calendar days of the effective date of the proposed Reliability Standard, and (ii) make any modifications to the list of identified facilities or documentation as to why no modifications were required (Part 2.3) within 60 days of completing the third party verification.

- *Requirement R3* – The Transmission Owner must make the required notification to the Transmission Operator within 7 calendar days of completion of performance under Requirement R2.[92]

- *Requirements R4 and R5* – Applicable Transmission Owners and Transmission Operators must complete the evaluation of threats and vulnerabilities and develop the security plan within 120 calendar days of completion of performance under Requirement R2.

- *Requirement R6* – Transmission Owners and Transmission Operators must (i) complete the third party review of the Requirement R4 evaluation and the Requirement R5 security plan (Parts 6.1 and 6.2) within 90 calendar days of completion of developing the Requirement R5 security plans, and (ii) make any modifications to the evaluation or security, or documentation as to why no modifications were required (Part 6.3) within 60 days of completing the third party review.

The standard drafting team concluded that the timeframes set forth in the Implementation Plan appropriately balances the urgency of implementing the requirements of the proposed Reliability Standard to protect the Bulk-Power System with providing entities sufficient time for effective implementation. While many entities are already taking steps to implement security measures, others may require time to develop internal processes, procedures, and budget

[92] Requirement R2 is complete when there is nothing left to do under the requirement. Specifically, if the verifier does not make any recommendations, then the Transmission Owner completes Requirement R2 once the verifier completes its verification. If the verifier makes one or more recommendations, the Transmission Owner only completes Requirement R2 when it has modified its identification of critical facilities consistent with the recommendations or documented its reasons for not doing so.

allocations to comply with proposed Reliability Standard CIP-014-1. In the interim, NERC will continue to use its existing reliability tools to work with industry to protect the security of the Bulk-Power System

VI. CONCLUSION

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

- the proposed Reliability Standard and associated elements included in Exhibit A, effective as proposed herein; and
- the proposed implementation plan included in Exhibit B;

Respectfully submitted,

/s/ Shamai Elstein

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

Counsel for the North American Electric Reliability Corporation

Date: May 23, 2014

Exhibit A

Proposed Reliability Standard

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-1

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner

shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified

Protection Professional (CPP) or Physical Security Professional (PSP) certification.

- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

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 during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three 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, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	May 13, 2014	Adopted by NERC Board of Trustees	

Guidelines and Technical Basis

Section 4 Applicability

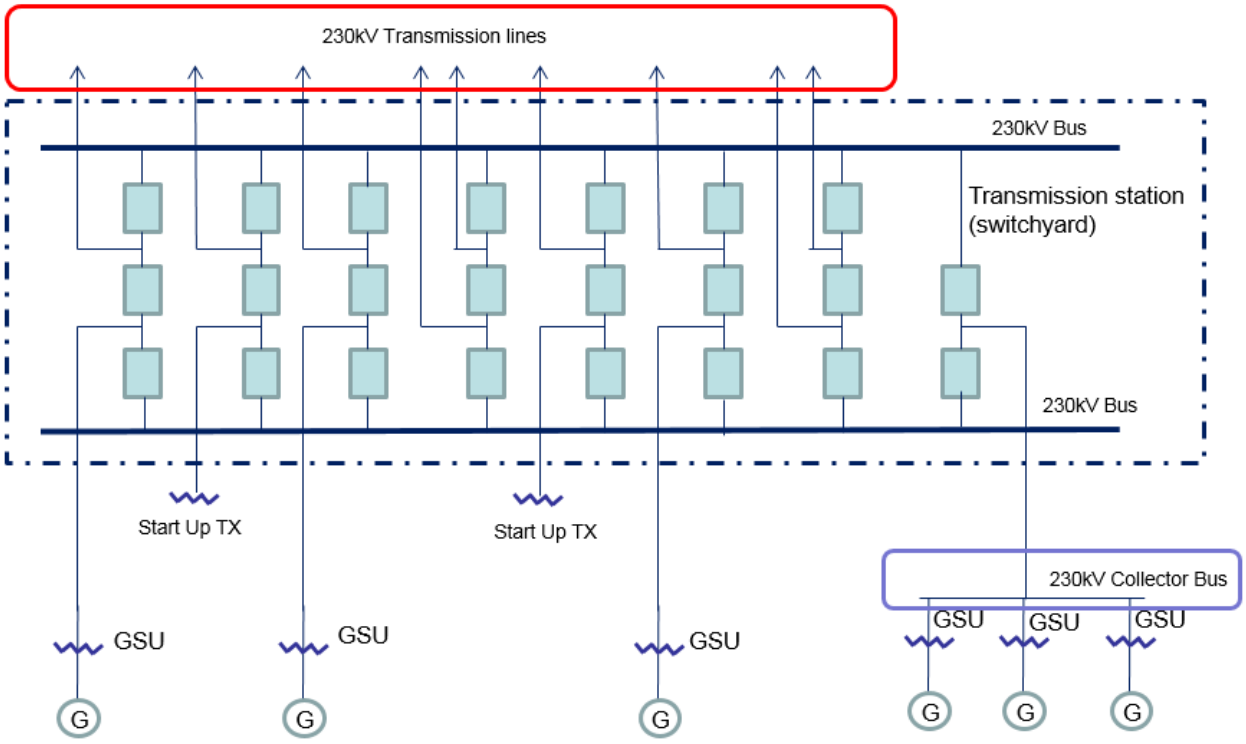
The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within

an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers that, if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014-1, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014-1 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014-1 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential widespread instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes widespread instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center “operationally controls” a Transmission station or Transmission substation when the control center’s electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.

2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.

- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk

assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

  Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to

Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*

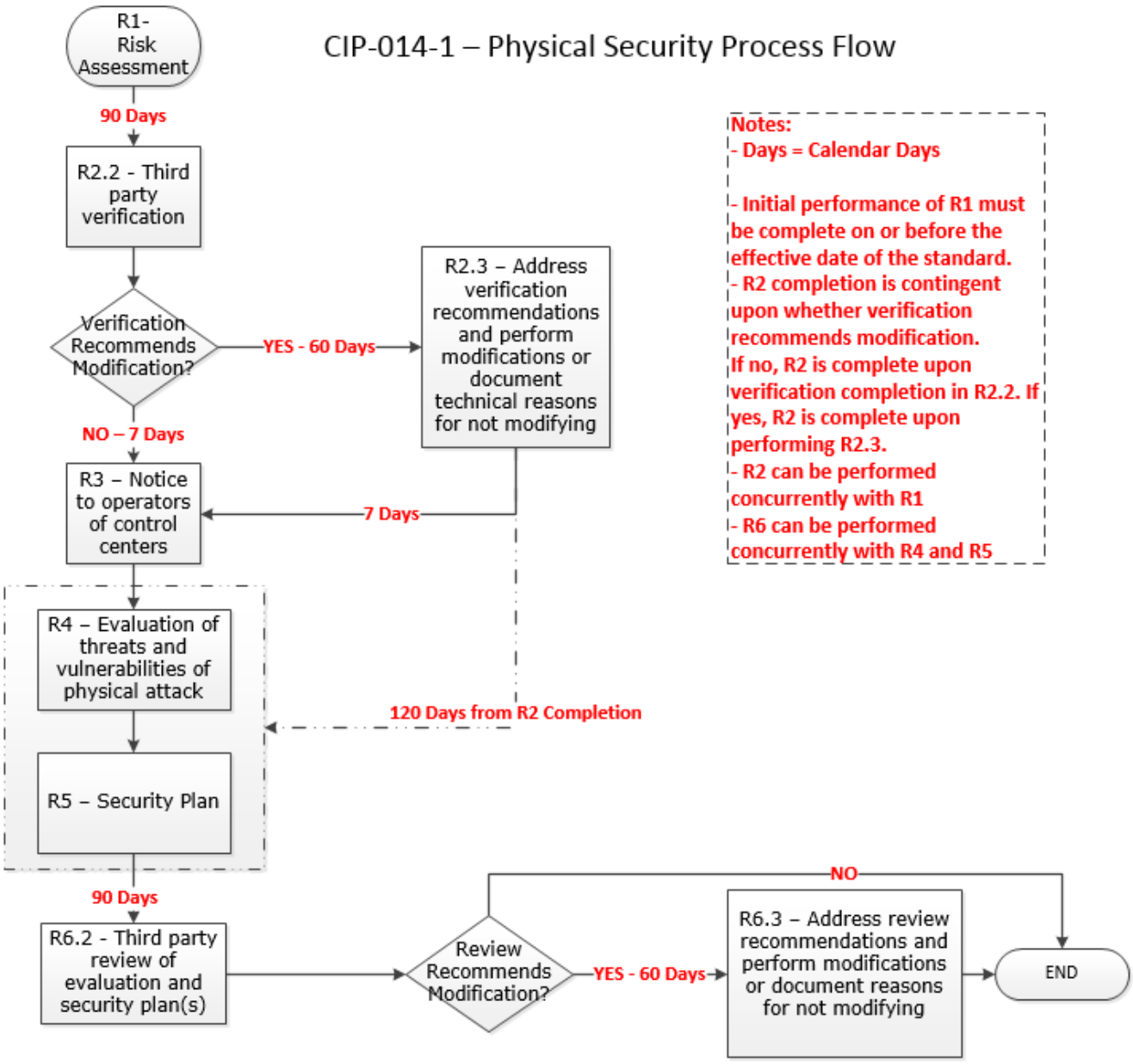
- *A governmental agency with physical security expertise.*

- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The

intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
NO
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

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 Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term “unaffiliated” means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term “unaffiliated” is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Project 2014-04

Approvals Requested
CIP-014-1 Physical Security

Prerequisite Approvals
None

Effective Date

New or Revised Standards
CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Standards for Retirement
None

Initial Performance of Periodic Requirements
The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard. Subsequent risk assessments shall be performed according to the timelines specified in CIP-014-1, Requirement R1.

The initial performance of CIP-014-1, Requirements R2 through R6, must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows:

- Requirement R2 shall be completed as follows:
    - Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard.
    - Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2.

- Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.
- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2.
- Requirement R6 shall be completed as follows:
    - Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5.
    - Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

Exhibit C

Order No. 672 Criteria

EXHIBIT C

Order No. 672 Criteria

In Order No. 672,[1] the Commission identified a number of criteria it will use to analyze Reliability Standards proposed for approval to ensure they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. The discussion below identifies these factors and explains how the proposed Reliability Standard has met or exceeded the criteria.

1. **Proposed Reliability Standards must be designed to achieve a specified reliability goal and must contain a technically sound means to achieve that goal.[2]**

Proposed Reliability Standard CIP-014-1 achieves the specific reliability goal of enhancing physical security measures for the most critical Bulk-Power System facilities and thereby lessening the overall vulnerability of the Bulk-Power System to physical attacks. The proposed Reliability Standard requires Transmission Owners and Transmission Operators to protect those critical Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Consistent with the Physical Security Order, the proposed Reliability Standard requires Transmission Owners to take the following steps to address the risks that physical attacks pose to the reliable operation of the Bulk-Power System:

1) Perform a risk assessment of their systems to identify (i) their critical Transmission stations and Transmission substations, and (ii) the primary control centers that operationally (i.e., physically) control the identified Transmission stations and Transmission substations.

---

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

[2] Order No. 672 at PP 321, 324.

2) Evaluate the potential threats and vulnerabilities of a physical attack to the facilities identified in the risk assessment.

3) Develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of the identified critical facilities.

Further, the proposed Reliability Standard requires Transmission Operators that operate primary control centers that operationally control any of the Transmission stations or substations identified by the Transmission Owner to also:

1) evaluate the potential threats and vulnerabilities of a physical attack to such primary control centers; and

2) develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of such primary control centers.

Additionally, proposed Reliability Standard CIP-014-1 includes requirements for: (i) the protection of sensitive or confidential information from public disclosure; (ii) third party verification of the identification of critical facilities as well as third party review of the evaluation of threats and vulnerabilities and the security plans; and (iii) the periodic reevaluation and revision of the identification of critical facilities, the evaluation of threats and vulnerabilities, and the security plans to help ensure their continued effectiveness.

2. Proposed Reliability Standards must be applicable only to users, owners and operators of the bulk power system, and must be clear and unambiguous as to what is required and who is required to comply.[3]

The proposed Reliability Standard is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed Reliability Standard applies to Transmission Owners and Transmission Operators. The proposed Reliability Standard clearly articulates the actions that such entities must take to comply with the standard.

---

[3] Order No. 672 at PP 322, 325.

3. A proposed Reliability Standard must include clear and understandable consequences and a range of penalties (monetary and/or non-monetary) for a violation.[4]

The Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") for the proposed Reliability Standard comport with NERC and Commission guidelines related to their assignment, as discussed further in Exhibit E. The assignment of the severity level for each VSL is consistent with the corresponding requirement and the VSLs should ensure uniformity and consistency in the determination of penalties. The VSLs do not use any ambiguous terminology, thereby supporting uniformity and consistency in the determination of similar penalties for similar violations. For these reasons, the proposed Reliability Standard includes clear and understandable consequences in accordance with Order No. 672.

4. A proposed Reliability Standard must identify clear and objective criterion or measure for compliance, so that it can be enforced in a consistent and non-preferential manner. [5]

The proposed Reliability Standard contains measures that support each requirement by clearly identifying what is required to demonstrate compliance. These measures help provide clarity regarding the manner in which the requirements will be enforced, and help ensure that the requirements will be enforced in a clear, consistent, and non-preferential manner and without prejudice to any party.

---

4 Order No. 672 at P 326.

5 Order No. 672 at P 327.

5. **Proposed Reliability Standards should achieve a reliability goal effectively and efficiently — but do not necessarily have to reflect "best practices" without regard to implementation cost or historical regional infrastructure design.[6]**

The proposed Reliability Standard achieves the reliability goal effectively and efficiently in accordance with Order No. 672. The proposed Reliability Standard clearly enumerates the responsibilities of applicable entities with respect to the identification and protection of critical Bulk-Power System facilities and provides entities the flexibility to tailor their processes and plans required under the standard to best suit the needs of their organization.

6. **Proposed Reliability Standards cannot be "lowest common denominator," *i.e.*, cannot reflect a compromise that does not adequately protect Bulk-Power System reliability. Proposed Reliability Standards can consider costs to implement for smaller entities, but not at consequences of less than excellence in operating system reliability.[7]**

The proposed Reliability Standard does not reflect a "lowest common denominator" approach. To the contrary, the proposed Reliability Standard contains significant benefits for the Bulk-Power System. The requirements of the proposed Reliability Standard help ensure that entities provide an adequate level of protection against physical attacks to critical facilities.

7. **Proposed Reliability Standards must be designed to apply throughout North America to the maximum extent achievable with a single Reliability Standard while not favoring one geographic area or regional model. It should take into account regional variations in the organization and corporate structures of transmission owners and operators, variations in generation fuel type and ownership patterns, and regional variations in market design if these affect the proposed Reliability Standard.[8]**

The proposed Reliability Standard applies throughout North America and does not favor one geographic area or regional model.

---

6 Order No. 672 at P 328.

7 Order No. 672 at P 329-30.

8 Order No. 672 at P 331.

8. Proposed Reliability Standards should cause no undue negative effect on competition or restriction of the grid beyond any restriction necessary for reliability.[9]

The proposed Reliability Standard has no undue negative impact on competition. The proposed Reliability Standard requires the same performance by each applicable entity. The standard does not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

9. The implementation time for the proposed Reliability Standard is reasonable.[10]

The proposed effective date for the standard is just and reasonable and appropriately balances the urgency in the need to implement the standard against the reasonableness of the time allowed for those who must comply to develop and implement the necessary procedures and policies. The proposed implementation period will allow applicable entities adequate time to meaningfully implement the requirements. The proposed effective date is explained in the proposed Implementation Plan, attached as Exhibit B.

10. The Reliability Standard was developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[11]

The proposed Reliability Standard was developed in accordance with NERC's Commission-approved, ANSI- accredited processes for developing and approving Reliability Standards. Exhibit F includes a summary of the Reliability Standard development proceedings, and details the processes followed to develop the Reliability Standards. These processes included, among other things, comment and balloting periods. Additionally, all meetings of the

---

9 Order No. 672 at P 332.

10 Order No. 672 at P 333.

11 Order No. 672 at P 334.

drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum and exceeded the required ballot pool approval levels.

11. NERC must explain any balancing of vital public interests in the development of proposed Reliability Standards.[12]

NERC has identified no competing public interests regarding the request for approval of the proposed Reliability Standard. No comments were received that indicated the proposed Reliability Standard conflicts with other vital public interests.

12. Proposed Reliability Standards must consider any other appropriate factors.[13]

No other negative factors relevant to whether the proposed Reliability Standard is just and reasonable were identified.

---

[12] Order No. 672 at P 335.

[13] Order No. 672 at P 323.

Exhibit D

Consideration of Directives

Consideration of Issues and Directives

Project 2014-04 - Physical Security

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
P.6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring Transmission Owners to perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. If the Transmission Owner does not have any Transmission stations or Transmission substations that meet the Medium

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		Impact rating, it is not subject to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the risk assessment is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed,	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
operated, and maintained, and the sophistication of recovery plans and inventory management.		
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1) resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4; (2) law enforcement

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		contact and coordination information; (3) a timeline for executing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to third party verifiers and reviewers and to protect or exempt sensitive or confidential information developed pursuant to the standard from public disclosure.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a	*Reliability Standards for Physical Security*	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated third party verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the verification shall either verify the Transmission Owner's risk assessment or include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The reviewing entity must be (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file the plan with the Reliability Standards for Commission review.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 Part 6.2.

Exhibit E

Analysis of Violation Risk Factors and Violation Security Levels

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-04: Physical Security

VRF and VSL Justifications for CIP-014-1

VRF and VSL Justifications – CIP-014-1, R1	
Proposed VRF	High
NERC VRF Discussion	Initial and subsequent risk assessments identify Transmission stations or Transmission substations that need to be assessed for threats and vulnerabilities and potential physical security measures. Since this is a Requirement in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the risk assessment periodicity and the identification of the primary control center that has operational control of Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-002-5.1 R1, which deals with categorizing cyber systems, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date;

VRF and VSL Justifications – CIP-014-1, R1	
	OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.
Proposed Moderate VSL	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.
Proposed High VSL	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in

VRF and VSL Justifications – CIP-014-1, R1	
	the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.
Proposed Severe VSL	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within

VRF and VSL Justifications – CIP-014-1, R1	
	an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if the risk assessment is not performed or if the risk assessment is not performed within required intervals.
FERC VSL G3 Violation Severity Level	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R1	
Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to submit perform a risk assessment.

VRF and VSL Justifications – CIP-014-1, R2	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party verification of initial and subsequent risk assessments provides reinforcement that the risk assessment was performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party verification including entities that may perform the verification, provisions for adding or removing Transmission stations and/or Transmission substations, and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but less than or equal to 100 calendar days following completion of Requirement R1;

VRF and VSL Justifications – CIP-014-1, R2	
	OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.
Proposed Moderate VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.
Proposed High VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to 120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by part 2.3.
Proposed Severe VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R2	
	verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party verification is not performed or if the verification is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based	The VSL is assigned for a single instance of failing to have an unaffiliated third party verification performed; or failing to perform the verification within prescribe timelines; or failing to implement procedures to protect information.

VRF and VSL Justifications – CIP-014-1, R2	
on A Single Violation, Not on A Cumulative Number of Violations	

VRF and VSL Justifications – CIP-014-1, R3	
Proposed VRF	Lower
NERC VRF Discussion	Notifying the Transmission Operator that it has operational control of a Transmission station or Transmission substation identified in Requirement R1 and verified in Requirement R2 is necessary so that the Transmission Operator may begin performance of subsequent physical security requirements for the primary control center. This is a requirement that is administrative in nature and in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. This justifies a Lower VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the notification of the Transmission Operator regarding the removal of a Transmission station or Transmission substation.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable INT-006-4 R6, which deals with notifying other entities so that Confirmed Interchange may be implemented, is assigned a Lower VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar

VRF and VSL Justifications – CIP-014-1, R3	
	days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.
Proposed Moderate VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.
Proposed High VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.
Proposed Severe VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1.

VRF and VSL Justifications – CIP-014-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if notification is not made subject to the conditions of the requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to make the appropriate notification.

VRF and VSL Justifications – CIP-014-1, R4	
Proposed VRF	Medium
NERC VRF Discussion	Performing an evaluation of potential threats and vulnerabilities of a physical attack to each of respective Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the evaluation of potential threats and vulnerabilities of a physical attack to Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-007-5 R2, which deals with a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets, is assigned a Medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	N/A

VRF and VSL Justifications – CIP-014-1, R4	
Proposed Moderate VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.
Proposed High VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.
Proposed Severe VSL	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failed to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R4	
Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failing to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R5	
Proposed VRF	High
NERC VRF Discussion	Development, implementation and execution of a documented physical security plan(s) that covers applicable Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the physical security plan for applicable Transmission stations, Transmission substations, or primary control centers.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-003-3 R4, which deals with implementing and documenting a program to identify, classify, and protect information associated with Critical Cyber Assets, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2;

VRF and VSL Justifications – CIP-014-1, R5	
	OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.
Proposed Moderate VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.
Proposed High VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.
Proposed Severe VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission

VRF and VSL Justifications – CIP-014-1, R5	
	station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include Parts 5.1 through 5.4 in the plan.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) or if the responsible entity failed to include any of the Requirement Parts 5.1-5.4.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level	The VSL is assigned for a single instance of failing to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and

VRF and VSL Justifications – CIP-014-1, R5	
Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	primary control center(s) or failing to include any of the Requirement Parts 5.1-5.4.

VRF and VSL Justifications – CIP-014-1, R6	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party review of the threat evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 provides reinforcement that these requirements were performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party review including entities that may perform the review, timelines for completing the review and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days;

VRF and VSL Justifications – CIP-014-1, R6	
	OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.
Proposed Moderate VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.
Proposed High VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not and modify or document the reason for not modifying the security plan(s) as specified in Part 6.3.
Proposed Severe VSL	The Responsible Entity failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R6	
	review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party review is not performed or if the review is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R6	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to have an unaffiliated third party review performed; or failing to perform the review within prescribe timelines; or failing to implement procedures to protect information.

Exhibit F

Summary of Development History and Record of Development

Summary of Development History

Summary of Development History

The development record for proposed Reliability Standard CIP-014-1 is summarized below.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived, in part, from the standard drafting team. For this project, the standard drafting team consisted of industry experts, all a diverse set of experiences. A roster of the standard drafting team members is included in Exhibit G.

II. Standard Development History

Following the issuance of the Physical Security Order, the NERC Standards Committee ("SC"), working with NERC staff, initiated Project 2014-04 Physical Security to develop a proposed Reliability Standard to satisfy FERC's directive to submit one or more physical security Reliability Standards by June 5, 2014 (i.e., within 90 days of the Physical Security Order).

A. Standard Processes Manual Waivers and Formation of Standards Drafting Team

To facilitate meeting the 90-day timeline, the NERC Standards Committee approved waivers to the Standard Processes Manual to shorten the comment and ballot periods for the Standards Authorization Request ("SAR") and draft Reliability Standard. The Standards Committee, working with NERC staff, also moved expeditiously to form a standard drafting team.

---

[1] Section 215(d) (2) of the Federal Power Act; 16 U.S.C. §824(d) (2) (2006).

Specifically, on March 12, 2014, the following actions were taken: (1) Standards Committee authorized solicitation of a drafting team; (2) the SC chair presented to the SC a proposal for waiver of certain provisions in the Standard Processes Manual to shorten the comment and ballot periods for the Standards Authorization Request ("SAR") and draft Reliability Standard; and (3) NERC posted solicitation of standard drafting team announcement, with nominations due Tuesday, March 18. On March 14, 2014 NERC posted notice of request for waiver of certain Standards Processes Manual provisions in accordance with Section 16 of the Standard Processes Manual. On March 21, 2014, the Standards Committee approved the requested waivers and appointed the standards drafting team.

B. Standard Authorization Request Development

NERC submitted a SAR to the SC on March 12, 2014. On March 21, 2014, the SC accepted the SAR and NERC posted the SAR for a seven-day informal comment period from March 21-28, 2014 in accordance with the SC-approved waiver of the Standard Processes Manual.

C. Technical Conference

On April 1, 2014, NERC held a technical conference to provide an opportunity for the standards drafting team, NERC, and industry participants to discuss issues related to applicability, identification of critical facilities, evaluation of threats and vulnerabilities, development and implementation of physical security plans, and a proposed implementation plan for the proposed Reliability Standard.

D. First Posting

Following standard drafting team meetings, NERC posted proposed Reliability Standard CIP-014-1 for a 15-day formal comment period from April 10, 2014 through April 24, 2014 in

accordance with the SC-approved waiver. On April 9, 2014, the Standards Committee authorized the posting of the proposed Reliability Standard for comment and ballot.

There were 136 sets of responses to the posting, including comments from approximately 240 different people from approximately 165 companies representing all 10 of the industry segments. The proposed Reliability Standard received a quorum of 88.60% and an approval of 82.07%.

The standard drafting team considered all comments and made the following non-substantive changes, among others, to the standard to incorporate stakeholder recommendations:

- Part 4.1.1 of the applicability section was changed to clarify that applicable Transmission Owners are those that own transmission stations or transmission substations meeting the criteria in 4.1.1.4 through 4.1.1.4.
- The exemption for covered by a security plans under Nuclear Regulatory Commission or Canadian Nuclear Safety Commission jurisdiction was changed to provide clarity on the scope of the exemption.
- Several additions were made to the guidance section of the standard to address stakeholder concerns.
- The standard drafting team drafted language in Requirement R2, Part 2.4, Requirement R6, Part 6.4 and Section 1.4 of the Compliance section of the standard to address confidentiality.
- The standard drafting team added language to the Guidelines and Technical Basis section to clarify the use of the term collector bus.
- Requirement R2, Part 2.2 was reworded to align with the intended applicable entity.
- A change was made to Requirement R3 to accurately state which primary control centers are included in the requirement.
- Changes were made to clarify factors to be considered by the responsible entity in Requirements R4 Parts 4.2 and 4.3.
- Requirement R5 was reworded to clarify the standard drafting team's intent for security plans to be developed within 120 days of completing Requirement R2 and executed according to the timeline specified in the security plan.

- Requirement R6, Part 6.1 was changed to clearly indicate that one or more of the criteria must be met.

- The standard drafting team added commentary in the Guidelines and Technical Basis section to address joint ownership.

E. Final Ballot

Proposed Reliability Standard CIP-014-1 was posted for a 5-day final ballot period from May 1, 2014 through May 5, 2014 in accordance with the SC-approved waiver. The proposed Reliability Standard received a quorum of 92.53% and an approval of 85.61%.

F. Board of Trustees Approval

Proposed Reliability Standard CIP-014-1 was approved by NERC Board of Trustees on May 13, 2014.

Record of Development

Project 2014-04 Physical Security

Related Files

Status:

The NERC Board of Trustees adopted the CIP-014-1 standard at their May 13, 2014 meeting and NERC staff is preparing the FERC filing.

Background:

This project will address the directives issued in the FERC Order on Reliability Standards for Physical Security Measures under Docket No. RD14-6-000 issued March 7, 2014. The Commission directed "The North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

Purpose/Industry Need:

From the Order: "Physical attacks to the Bulk-Power System can adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures. However, the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks on the Bulk-Power System. Therefore, to carry out section 215 of the FPA and to provide for the reliable operation of the Bulk-Power System, the Commission directs the ERO to develop and file for approval proposed Reliability Standards that address threats and vulnerabilities to the physical security of critical facilities on the Bulk-Power System. Such Reliability Standards will enhance the Commission's ability to assure the public that critical facilities are reasonably protected against physical attacks."

Draft	Actions	Dates	Results	Consideration of Comments
CIP-014-1 Clean (21) | Redline to Last Posted (22) Implementation Plan (23)	Final Ballot Info>> (29) Vote>>	05/01/14 - 05/05/14	Summary>> (30) Ballot Results>> (31)	

Supporting Materials: Consideration of Issues and Directives Clean (24) | Redline to Last Posted (25) VRF/VSL Justifications (26) Draft RSAW Clean (27) | Redline to Last Posted (28)				
CIP-014-1 (7) Implementation Plan (8) **Supporting Materials:** Project Overview (9) FAQ (10) Unofficial Comment Form (Word) (11) Consideration of Issues and Directives (12) Draft RSAW (13)	Initial Ballot and Non-Binding Poll Info>> (14) Vote>>	04/20/14 - 04/24/14	Summary>> (16) Ballot Results>> (17) Non-Binding Poll Results>> (18)	Consideration of Comments>> (20)
	Comment Period Info>> (15) Submit Comments>>	04/10/14 - 04/24/14	Comments Received>> (19)	
	Join Ballot Pool>>	04/10/14 - 04/19/14		
	Please send feedback on the draft RSAW to: RSAWfeedback@nerc.net	04/10/14 - 04/24/14		
Standards Authorization Request (3)	Comment Period Info>> (5) Submit Comments>>	03/21/14 – 03/28/14	Comments Received>> (6)	

Supporting Materials: Unofficial Comment Form (Word) (4)	Join Ballot Pool>>			
Supporting Materials: Nomination Form (Word) (1)	Nomination Period Info>> (2) Submit Nominations>>	03/12/14 - 03/18/14		

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2014-04 Physical Security Standard Drafting Team

Please complete the electronic nomination form as soon as possible, but no later than **March 18, 2014.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form. If you have any questions, please contact Stephen Crutchfield.

By submitting a nomination form, you are indicating your willingness and agreement to actively participate in the drafting team meetings (see dates of technical conference and first drafting team meeting below) if appointed by the Standards Committee. If appointed, you are expected to attend most of the face-to-face drafting team meetings as well as participate in all the team meetings held via conference calls. Failure to do so may result in your removal from the drafting team.

Background Information

Nominations are being sought for the Project 2014-04 Physical Security Standard Drafting Team (SDT). On March 7, 2014, FERC issued an Order, directing NERC to develop a new Reliability Standard to address concerns about the physical security of the Bulk-Power System. From the order:

> "The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

Potential SDT members should have experience in physical security programmatic design, risk assessments, evaluations, management, and identification of critical transmission substations and control centers, rather than the execution of physical security plan mitigation measures. In addition, compliance, legal, regulatory, and technical writing are desired. Previous drafting team experience and/or experience with development of standards is beneficial, but not required.

The expected time commitment for this team is aggressive because of directives with a deadline associated with them. The SDT is expected to meet in person for up to three full three-day meetings

during the project which is anticipated to last 90 days, with additional conference calls between face-to-face meetings as necessary to meet the aggressive project schedule. The first technical conference will be held in Atlanta on April 1, 2014 and the new drafting team will meet immediately following, April 2-4, 2014. SDT members are expected to attend both events.

Please provide the following information for the nominee:	
Name:	
Title:	
Organization:	
Address:	
Telephone:	
Email:	

Please briefly describe the nominee's experience and qualifications to serve on the selected project:

If you are currently a member of any NERC SAR or standard drafting team(s), please list each team here:

☐ Not currently on any active SAR or standard drafting team.

☐ Currently a member of the following SAR or standard drafting team(s):

If you previously worked on any NERC SAR or standard drafting team(s)s, please identify the team(s):

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following SAR or standard drafting team(s):

Select each NERC Region in which you have experience relevant to Project 2014-04:

☐ ERCOT	☐ NPCC	☐ SPP
☐ FRCC	☐ RFC	☐ WECC
☐ MRO	☐ SERC	☐ NA – Not Applicable

Select each Industry Segment that you represent:	
☐	1 — Transmission Owners
☐	2 — RTOs, ISOs
☐	3 — Load-serving Entities
☐	4 — Transmission-dependent Utilities
☐	5 — Electric Generators
☐	6 — Electricity Brokers, Aggregators, and Marketers
☐	7 — Large Electricity End Users
☐	8 — Small Electricity End Users
☐	9 — Federal, State, and Provincial Regulatory or other Government Entities
☐	10 — Regional Reliability Organizations and Regional Entities
☐	NA – Not Applicable

Select each Function[1] in which you have current or prior expertise:	
☐ Balancing Authority	☐ Transmission Operator
☐ Compliance Enforcement Authority	☐ Transmission Owner
☐ Distribution Provider	☐ Transmission Planner
☐ Generator Operator	☐ Transmission Service Provider
☐ Generator Owner	☐ Purchasing-selling Entity
☐ Interchange Authority	☐ Reliability Coordinator
☐ Load-serving Entity	☐ Reliability Assurer
☐ Market Operator	☐ Resource Planner
☐ Planning Coordinator	

Provide the names and contact information for two references who could attest to your technical qualifications and your ability to work well in a group:			
Name:		Telephone:	
Organization:		Email:	

[1] These functions are defined in the NERC Functional Model, which is available on the NERC web site.

Name:		Telephone:	
Organization:		Email:	
Provide the names and contact information of your immediate supervisor or a member of your management who can confirm your organization's willingness to support your active participation.			
Name:		Telephone:	
Title:		Email:	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security Standard Drafting Team

Nomination Period Now Open through March 18, 2014

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

Link to Official Nomination Form
Link to Word Version of Nomination Form

Nominations are being sought for the Project 2014-04 Physical Security Standard Drafting Team (SDT). On March 7, 2014, FERC issued an Order, directing NERC to develop a new Reliability Standard to address concerns about the physical security of the Bulk-Power System. From the order:

> "The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

Potential SDT members should have experience in physical security programmatic design, risk assessments, evaluations, management, and identification of critical transmission substations and control centers, rather than the execution of physical security plan mitigation measures. In addition, compliance, legal, regulatory, and technical writing are desired. Previous drafting team experience and/or experience with development of standards is beneficial, but not required.

The expected time commitment for this team is aggressive because of directives with a deadline associated with them. The SDT is expected to meet in person for up to three full three-day meetings during the project which is anticipated to last 90 days, with additional conference calls between face-to-face meetings as necessary to meet the aggressive project schedule. The first technical conference will be held in Atlanta on April 1, 2014 and the new drafting team will meet immediately following, April 2-4, 2014. SDT members are expected to attend both events.

Submitting a Nomination

If you are interested in serving on the SDT, please complete the official nomination form by **March 18, 2013**. The nomination form should be submitted describing the individual's experience or qualifications related to the project.

An unofficial Word version of the nomination form is also posted on the Standard Drafting Team Vacancies page.

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Standards Authorization Request Form

When completed, email this form to:
Barbara.Nutter@nerc.net

For questions about this form or for assistance in completing the form, call Barb Nutter at 404-446-9692.

NERC welcomes suggestions for improving the reliability of the Bulk-Power System through improved Reliability Standards. Please use this form to submit your proposal for a new NERC Reliability Standard or a revision to an existing standard.

Request to propose a new or a revision to a Reliability Standard			
Proposed Standard:	Project 2014-04 Physical Security Reliability Standard(s)		
Date Submitted:	March 12, 2014		
SAR Requester Information			
Name:	Stephen Crutchfield		
Organization:	NERC Staff		
Telephone:	609-651-9455	E-mail:	Stephen.crutchfield@nerc.net
SAR Type (Check as many as applicable)			
☒ New Standard		☐ Withdrawal of existing Standard	
☐ Revision to existing Standard		☐ Urgent Action	

SAR Information
Industry Need (What is the industry problem this request is trying to solve?):
On March 7, 2014, FERC issued an order directing the ERO to develop a standard to address the physical security of critical facilities on the Bulk-Power System. In the order, FERC stated: "The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order." *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 at P 1 (2014) ("FERC Order").
SAR Information
Purpose or Goal (How does this request propose to address the problem described above?):
The primary goal of this SAR is to allow the Standard Drafting Team (SDT) for Project 2014-04, Physical Security to develop a standard(s) to address the directives of the March 7, 2014 FERC Order and to ensure consistency within the NERC body of Reliability Standards.
Identify the Objectives of the proposed standard's requirements (What specific reliability deliverables are required to achieve the goal?):
Provide clear, unambiguous requirements and standard(s) to address the directives in the March 7, 2014 FERC Order regarding the physical security of critical facilities on the Bulk-Power System.
Brief Description (Provide a paragraph that describes the scope of this standard action.)
The SDT shall develop standard requirements, Violation Risk Factors, Violation Severity Levels, and implementation plan and shall work with compliance on an accompanying RSAW to address each of the directives in the March 7, 2014 FERC Order.

SAR Information
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)
The SDTs execution of this SAR requires the SDT to address each of the FERC directives in the deadline required by the Order. The reliability assessment and justification is also set forth in the March 7, 2014 FERC Order. The March 7, 2014 FERC Order is incorporated in its entirety into this SAR, so as not to unnecessarily repeat or paraphrase the substance of the Order. There are no market interface impacts resulting from the standard action on physical security.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☐ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☐ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
☐ Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐ Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐ Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.

Reliability Functions		
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☐	Distribution Provider	Delivers electrical energy to the End-use customer.
☐	Generator Owner	Owns and maintains generation facilities.
☐	Generator Operator	Operates generation unit(s) to provide real and reactive power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.

Reliability and Market Interface Principles	
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A reliability standard shall not give any market participant an unfair competitive advantage.	Yes
2. A reliability standard shall neither mandate nor prohibit any specific market structure.	Yes
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.	Yes
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.	Yes

Related Standards	
Standard No.	Explanation
CIP-006-5 CIP-008-5 CIP-009-5	Review to ensure no language and terminology inconsistency with requirements developed under this project.

Related Standards	

Related SARs	
SAR ID	Explanation
N/A	N/A

Regional Variances	
Region	Explanation
ERCOT	N/A
FRCC	N/A
MRO	N/A
NPCC	N/A
RFC	N/A
SERC	N/A
SPP	N/A
WECC	N/A

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2014-04 Physical Security

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the draft Physical Security Standard Authorization Request (SAR). The electronic comment form must be completed by **8:00 p.m. Eastern on March 28, 2014**.

If you have questions please contact Stephen Crutchfield via email or by telephone at 609-651-9455.

The project page may be accessed by clicking here.

Background Information

On March 7, 2014, FERC issued an order directing the ERO to develop a standard to address the physical security of critical facilities on the Bulk-Power System. In the order, FERC stated:

"The Commission directs the North American Electric Reliability Corporation (NERC), as the Commission-certified Electric Reliability Organization (ERO), to submit for approval one or more Reliability Standards that will require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the Bulk-Power System. The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. The Commission directs NERC to submit the proposed Reliability Standards to the Commission within 90 days of the date of this order."

You do not have to answer all questions. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained.

Questions

1. Do you agree with the scope and contents of the SAR? If not, please provide specific comments and suggestions for SDT consideration.

   ☐ Yes
   ☐ No
   Comments:

2. Are you aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project? If yes, please identify the Regional Variance.

   ☐ Yes
   ☐ No
   Comments:

3. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard(s)? If yes, please identify the jurisdiction and specific regulatory requirements.

   ☐ Yes
   ☐ No
   Comments:

4. Are there any other concerns with this SAR?

   ☐ Yes
   ☐ No
   Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security Standards Authorization Request

Informal Comment Period: March 21-28, 2014

Ballot Pools Forming Now

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

Now Available

A 7-day informal comment period for the **Project 2014-04 Physical Security Standards Authorization Request** is open through **8 p.m. Eastern on Friday, March 28, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455.

Background information for this project can be found on the project page.

Instructions for Commenting

Please use the electronic form to submit comments on the revised definition. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for Project 2014-04 – Physical Security and the associated non-binding poll on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated VRFs and VSLs. Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Initial Ballot: bp-2014-04_CIP-014-1_in@nerc.com
Non-Binding poll: bp-2014-04_CIP-014-1_NB_in@nerc.com

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Comment Summary

Project 2014-04 Physical Security

The Project 2014-04 Physical Security Standard Authorization Request (SAR) was posted for a 7-day public comment period from March 21, 2014 through March 28, 2014. Stakeholders were asked to provide feedback on the standards and associated documents through a special electronic comment form.

Index to Questions, Comments, and Responses

1. **Do you agree with the scope and contents of the SAR? If not, please provide specific comments and suggestions for SDT consideration.** 10
2. **Are you aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project? If yes, please identify the Regional Variance** 30
3. **Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard(s)? If yes, please identify the jurisdiction and specific regulatory requirements.**.....35
4. **Are there any other concerns with this SAR?** 40

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Lee Pedowicz	Northeast Power Coordinting Council										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	David Burke	Orange and Rockland Utilities Inc.	NPCC	3
3.	Greg Campoli	New Yorki Independent System Operator	NPCC	2
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1
5.	Ben Wu	Orange and Rockland Utilities Inc.	NPCC	1
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10
7.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Ayesha Sabouba	Hydro One Networks, Inc.	NPCC	1
10.	Mark Kenny	Northeast Utilities	NPCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Christina Koncz	PSEG Power LLC	NPCC	5
12.	Helen Lainis	Independent Electricity System Operator	NPCC	2
13.	Michael Lombardi	Northeast Power Coordinating Council	NPCC	10
14.	Alan MacNaughton	New Brunswick Power Corporation	NPCC	9
15.	Bruce Metruck	New York Power Authority	NPCC	6
16.	Silvia Parada Mitchell	NextEra energy, LLC	NPCC	5
17.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
18.	Robert Pellegrini	The United Illuminating Company	NPCC	1
19.	Si Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
20.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
21.	Wayne Sipperly	New York Power Authority	NPCC	5

2.	Group	Richard Hoag	FirstEnergy Corp.	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	William Smith	FirstEnergy Corp		1
2.	Cindy Stewart	FirstEnergy Corp		3
3.	Doug Hohlbaugh	Ohio Edison		4
4.	Ken Dresner	FirstEnergy Solutions		5
5.	Kevin Querry	FirstEnergy Solutions		6
6.	Richard Hoag	FirstEnergy Corp		NA

3.	Group	Jared Shakespeare	Peak Reliability	X									

No Additional Responses.

4.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Larry Nash	Dominion	SERC	1, 3, 5, 6
2.	Mike Garton	Dominion	NPCC	5, 6
3.	Randi Heise	Dominion	MRO	6
4.	Louis Slade	Dominion	RFC	5, 6

5.	Group	Marcus Pelt	Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company;	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Southern Company Generation and Energy Marketing										
No Additional Responses													
6.	Group	Colby Bellville	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Lee Schuster	Duke Energy	FRCC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

7.	Group	Dennis Chastain	Tennessee Valley Authority	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	DeWayne Scott		SERC	1
2.	Ian Grant		SERC	3
3.	David Thompson		SERC	5
4.	Marjorie Parsons		SERC	6

8.	Group	Greg Campoli	ISO RTO standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Lori Spence	MISO	MRO	2
2.	Cheryl Moseley	ERCOT	ERCOT	2
3.	Matt Goldberg	ISONE	NPCC	2
4.	Charles Yeung	SPP	SPP	2
5.	Ben Li	IESO	NPCC	2
6.	Tom Bowe	PJM	RFC	2
7.	Ali Miremadi	CAISO	WECC	2

9.	Group	Warren Cross	ACES Standards Collaborators						X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Old Dominion Electric Cooperative		SERC	3, 4
2.	Brazos Electric Power Cooperative		ERCOT	1, 5
3.	Golden Spread Electric Cooperative		ERCOT	5
4.	Sunflower Electric Power Corporation		SPP	1

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5. Great River Energy			MRO	1, 3, 5, 6									
6. Hoosier Energy Rural Electric Cooperative			RFC	1									
10.	Group	Robert Rhodes	SPP Standards Review Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Matthew Bordelon	Cleco Power	SPP	1, 3, 5, 6
2.	Chris Carlson	Grand River Dam Authority	SPP	1
3.	Phil Clark	Grand River Dam Authority	SPP	1
4.	Michelle Corley	Cleco Power	SPP	1, 3, 5, 6
5.	Tony Eddleman	Nebraska Public Power District	MRO	1, 3, 5
6.	Louis Guidry	Cleco Power	SPP	1, 3, 5, 6
7.	Robert Hirchak	Cleco Power	SPP	1, 3, 5, 6
8.	Kyle McMenamin	Xcel Energy	SPP	1, 3, 5, 6
9.	Fred Meyer	Empire Electric District	SPP	1, 3, 5
10.	Shannon Mickens	Southwest Power Pool	SPP	2
11.	Pat Morrill	Kansas City Board of Public Utilities	SPP	3
12.	James Nail	City of Independence, MO	SPP	3
13.	Dennis Sauriol	American Electric Power	SERC	1, 3, 5
14.	Don Schmit	Nebraska Public Power District	MRO	1, 3, 5
15.	Angela Summer	Southwestern Power Administration	SPP	1
16.	Tracey Stewart	Southwestern Power Administration	SPP	1
17.	Ellen Watkins	Sunflower Electric Power Corporation	SPP	1

11.	Group	Andrea Jessup	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jeff Millennor	Physical Security	WECC	1
2.	Richard Becker	Substation Engineering	WECC	1

12.	Group	William Harris	Foundation for Resilient Societies								X		
No Additional Responses													
13.	Individual	Dan Inman	Minnkota Power Cooperative	X									
14.	Individual	Oliver Burke	Entergy Services, Inc.	X									
15.	Individual	Peter Scalici	NPCC										

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
16.	Individual	Debra R Warner	Self								X		
17.	Individual	Steve Hamburg	Encari	X									
18.	Individual	Chris Scanlon	Exelon	X		X	X	X	X				
19.	Individual	Harold Dalson	Consumers Energy		X	X	X						
20.	Individual	Kevin Weber	Entergy Services, Inc.	X		X							
21.	Individual	Tim Reagan	Ameren	X									
22.	Individual	Gary Pagel	Idaho Power Co.	X									
23.	Individual	Karen Webb	City of Tallahassee - Electric Utility					X					
24.	Individual	David Kiguel	David Kiguel								X		
25.	Individual	Ralph Meyer	The Empire District Electric Company	X		X		X					
26.	Individual	mike kidwell	the empire district electric company					X					
27.	Individual	Kalem Long	The Empire District Electric Company			X							
28.	Individual	Megan Wagner	Westar Energy	X		X	X	X	X				
29.	Individual	Aaron Staley	Orlando Utilities Commission	X		X		X					
30.	Individual	Michelle R D'Antuono	Occidental Energy Ventures Corp.			X		X		X			
31.	Individual	Martyn Turner	LCRA Transmission Services Corporation	X									
32.	Individual	Shannon Fair	Colorado Springs Utilities	X				X					
33.	Individual	Bill Fowler	City of Tallahassee			X							
34.	Individual	Scott Langston	City of Tallahassee	X									
35.	Individual	Michael Falvo	Independent Electricity System Operator		X								
36.	Individual	Joseph DePoorter	Madison Gas and Electric Company				X						
37.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
38.	Individual	Thomas Foltz	American Electric Power	X		X		X	X				
39.	Individual	David Ramkalawan	OPG					X					
40.	Individual	Lisa Martin	City of Austin dba Austin Energy	X		X	X	X	X				
41.	Individual	Ayesha Sabouba	Hydro One	X		X							

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
42.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
43.	Individual	Bill Temple	Northeast Utilities	X									
44.	Individual	Amy Casuscelli	Xcel Energy Inc.	X			X	X	X				
45.	Individual	Brian Evans-Mongeon	Utility Services, Inc								X		
46.	Individual	Tony Eddleman	Nebraska Public Power District	X		X		X					
47.	Individual	David Jendras	Ameren	X		X		X	X				
48.	Individual	Alan MacNaughton	New Brunswick Power Corporation	X	X	X		X					
49.	Individual	Sergio Banuelos	Tri-State Generation and Transmission Association, Inc.	X		X		X					
50.	Individual	Bob Steiger	Salt River Project	X		X		X	X				
51.	Individual	Jennifer Flandermeyer	Kansas City Power & Light	X		X		X	X				

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Organization	Agree	Supporting Comments of "Entity Name"
NPCC	Agree	
Ameren	Agree	Eric ScottAmeren

1. Do you agree with the scope and contents of the SAR? If not, please provide specific comments and suggestions for SDT consideration.

Organization	Yes or No	Question 1 Comment
Tennessee Valley Authority	No	The SDT should consider expanding the applicable entities identified in the SAR. For instance, the type of system risk assessment that FERC suggests in the March 7 order is likely to be conducted by the Transmission Planner / Planning Authority. The Reliability Coordinator might also have information that is pertinent to such a risk assessment from a wide area operations viewpoint. In the event that a generating plant or associated transmission switchyard is identified as a critical facility, the Generator Owner / Generator Operator should be involved in the process of evaluating potential threats and vulnerabilities to those facilities and the development and implementation of the security plan.The following standards should be added to the list of relavent standards to be reviewed by the SDT: CIP-002-3 (R1, R1.2);CIP-002-5.1 (R1 and Attachment 1, Impact Rating Criteria for BES Cyber Systems);FAC-010-2.1 (addresses the Planning Authority(Coordinator) methodology for identifying IROLs);FAC-011-2 (addresses the Reliability Coordinator methodology for identifying IROLs;FAC-014-2 (R5.1.1, use of “critical” in reference to Facility(ies) used to derive an IROL);IRO-002-2 (R5, use of “critical” in reference to BES elements);IRO-003-2 (R2, use of “critical facilities”);IRO-008-1 / IRO-009-1 / IRO-010-1a / TOP-001-2 / TOP-004-2 (the purpose statement for these standards includes “to prevent instability, uncontrolled separation, or cascading outages”, which is language used in the FERC order for identifying critical facilities);TPL-001-4 (R6, addresses the criteria or methodology used by the TP and PC to identify System instability)The SDT should also consider the definition of Interconnection Reliability Operating Limit (IROL) in

Organization	Yes or No	Question 1 Comment
		development of the physical security standard. This definition includes language used in the FERC order to describe a "critical facility".
SPP Standards Review Group	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be figured out. Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. We need to come to some resolution of terms in order to determine where the playing field lies.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. Why were they left out? Also, BAs and RCs are not listed as applicable entities. Shouldn't they be included also? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.
Bonneville Power Administration	No	BPA believes that generally, this type of standard would be useful to the electric industry. The biggest issue for the SAR is the scope is loosely defined. As described, the objective of protecting critical facilities of the BES is stated too broadly and it is not apparent what countermeasures would be considered adequate or sufficient. ..."Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities." BPA believes that there are also many questions and issues to resolve to get to an acceptable level of risk that is lower than what may be in place today, and the 90 day drafting

Organization	Yes or No	Question 1 Comment
		period may not be long enough to define adequate expectations. A phased development approach may be more conducive to obtaining the benefits desired - - for example, assessment and ranking standard(s) first followed by mitigation options and requirements standard(s) to address gaps identified by the assessment.
Foundation for Resilient Societies	No	SAR Only includes Transmission Owners and Operators. This does not include all critical facilities.
Self	No	After reviewing the SAR, where in the Reliability and Market Interface Principles the box 5 for facilities for communication monitoring and control are referenced, I believe that the Reliability Coordinator Function should have been checked also. Is this an oversight in the draft SAR?
Consumers Energy	No	The information contained in the attached PDF files seems very vague and open ended. I would specifically point ot page 2, under the Industry Need section 2nd paragraph, line 3:"will require certain registered entities" I believe the term certain should be changed to a term of greater focus such as "entities that meet a predetermined set of criteria used to determine local, regional, and national criticality."2nd paragraph, line 8:"may compromise", again I think there needs to be some "degree" of compromise contained in this section. Example a chunk of stolen copper, to some degree can compromise a system, just as a VBIED can compromise a system. In areas where a "compromise" could cause a consequence at a local level, and the primary identified risk is trespass and copper theft this SAR as written suggests we 'Mitigate" the risk of compromise, not the cause of compromise coupled with the identified consequence of the compromise. An owner should have the ability to identify the risk, the consequence, and the mitigations to "prevent" that type of compromise in areas or sections of the system that would impact local, and perhaps to some degree regional consequences. If in fact an owner has assets that

Organization	Yes or No	Question 1 Comment
		could, if compromised cause cascading events that impact areas outside of their system operational area, those assets would show a greater consequence area and would require a greater level of protection.
City of Tallahassee - Electric Utility	No	TAL has concerns with the expedited nature of the timeline. The issue of physical security has been known for quite some time. The timeline of this directive appears to be solely in reaction to the publishing of the Metcalf incident. This directive and expedited time line precludes the dialog from occurring that needs to take place to truly understand what is expected to satisfy the Commission's desires. TAL believes this directive will yield a standard that is difficult to enforce with little benefit to the large majority of the BES. Additionally, the publicizing of certain "known" studies indicating that as little as nine substations will cause a large blackout is problematic.
David Kiguel	No	1. The SAR should include other entities in the applicability section such as Generator Owners (GO) and Generator Operators (GOP). The FERC Directive indicates that the proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of theBulk-Power System. It is clear that GOs and GOPs also own and operate Bulk-Power System facilities. 2. The FERC Directive requires that a risk assessment of the systems to identify their "critical facilities" be performed. In many cases, the entity that would be in the best position to perform such assessment would be the RC or the PC. It is suggested one of these be added in the SAR so the SDT can assign this responsibility to one of these functional entities. 3. The FERC Directive contains a requirement that NERC includes in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential informationbut still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability

Organization	Yes or No	Question 1 Comment
		Standards. Review and inspect such information on the part of the Commission should be limited to entities that are under FERC's jurisdiction. Canadian and/or Mexican data should be provided to regulators in the respective jurisdiction only, unless aggregated in a manner that will not allow to identify individual entities.
The Empire District Electric Company	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be addressed so that the expectation of a critical facility is clear to entities. Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. There needs to be some resolution of terms in order to determine where FERC's concern is focused so that a proper solution can be devloped.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. These may be considered? Also, BAs and RCs are not listed as applicable entities-shouldn't they be included also as they have the overall ability to direct and control the BES? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.
the empire district electric company	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be figured out.

Organization	Yes or No	Question 1 Comment
		Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. We need to come to some resolution of terms in order to determine where the playing field lies.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. Why were they left out? Also, BAs and RCs are not listed as applicable entities. Shouldn't they be included also? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.
The Empire District Electric Company	No	The FERC order references facilities which we assume are then tied to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. How does one then determine the list of 'critical' facilities if that definition no longer exists? The distinction between critical facility and critical asset needs to be figured out. Also, FERC's interpretation of 'facility' isn't consistent with the NERC definition of Facility since FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. We need to come to some resolution of terms in order to determine where the playing field lies.The SAR refers only to TOs and TOPs with no reference to GOs and GOPs who also own and operate facilities on the BES. Why were they left out? Also, BAs and RCs are not listed as applicable entities. Shouldn't they be included also? Will FERC accept a standard without these entities being included?While the SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT.

Organization	Yes or No	Question 1 Comment
Westar Energy	No	The SAR refers only to TOs and TOPs with no reference to other registered functions. Should the applicability be expanded to include all registered functions who own and operate facilities on the BES and would be involved in the assessment process?
Colorado Springs Utilities	No	The SAR refers to the entire order being incorporated into the SAR we suggest that the SDT specifically list each of the directives in bullet fashion in the SAR such that the stakeholders can be assured that they have all been included and will then be addressed by the SDT. We would recommend Brightline Criteria For the identification of critical Bulk Electric System Facilities, based on either the Transmission Planning Standard TPL-004a or identification of the largest single contingency for each interconnection. If we need a single number, including only Facilities that provide or control over 3000 MW of generation or transmission or transmission operating at 300 kV and above. Case-specific analysis and consideration of exceptions will be needed, but we need to start with a high lower limit.
City of Tallahassee	No	TAL has concerns with the expedited nature of the timeline. The issue of physical security has been known for quite some time. The timeline of this directive appears to be solely in reaction to the publishing of the Metcalf incident. This directive and expedited time line precludes the dialog from occurring that needs to take place to truly understand what is expected to satisfy the Commission's desires. TAL believes this directive will yield a standard that is difficult to enforce with little benefit to the large majority of the BES. Additionally, the publicizing of certain "known" studies indicating that as little as nine substations will cause a large blackout is problematic.

Organization	Yes or No	Question 1 Comment
City of Tallahassee	No	TAL has concerns with the expedited nature of the timeline. The issue of physical security has been known for quite some time. The timeline of this directive appears to be solely in reaction to the publishing of the Metcalf incident. This directive and expedited timeline precludes the dialog from occurring that needs to take place to truly understand what is expected to satisfy the Commission's desires. TAL believes this directive will yield a standard that is difficult to enforce with little benefit to the large majority of the BES. Additionally, the publicizing of certain "known" studies indicating that as little as nine substations will cause a large blackout is problematic.
Independent Electricity System Operator	No	We generally agree with the purpose and scope of the SAR, but we disagree with the applicability.The purpose of this project is develop a standard that will require owners and/or operators of the Bulkâ€Power System, as appropriate, to identify facilities on the Bulkâ€Power System that are critical to the reliable operation of the Bulkâ€Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. We interpret the "identify facilities" part in the first sentence to mean assessing the reliability impacts of the facilities which, if deemed inoperable, can result in instability, uncontrolled separation or cascading failures on the Bulk-Power System. Such tasks will thus require power system analysis not unlike the type required for transmission planning assessment, with a focus on losing the all the facilities at a location (e.g. a transmission substation, a large power plant, a right of way, etc.). These tasks will likely involve the Planning Coordinator and/or the Reliability Coordinator.This interpretation is also inferred from Para. 6 and Footnote #6 of the Order. Below is an excerpt of Para. 6 and FN#6:6. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their

Organization	Yes or No	Question 1 Comment
		systems to identify their “critical facilities.” A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. (FN#6) Instead, the Commission is directing NERC to develop Reliability Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System.FN#6 says: However, the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers.Two key points:a. FN#6 clearly indicates that it is the Commission’s expectation that control centres are critical facilities. The most critical control centres are those of the RCs. Hence, the RC’s inclusion in the standard appears to be very likely.b. Para 6 suggests that critical facilities are necessary those that if rendered not operable, they have wide-area reliability impact associated with instability, uncontrolled separation or cascading failures. We fully expect the standard to require responsible entities to have a process and criteria in place with which to identify the critical facilities from a wide-area reliability impact point of view. Such tasks will involve reliability assessments that are normally performed by the Planning Coordinator and Reliability Coordinator, depending on the time frame. In the Applicability Section, however, neither the PC’s nor the RC’s box is checked. We suggest the SAR be revised to include at least these two entities as potential applicable entities so that the drafting team does not foreclose the possibility that reliability assessments need to be conducted to aid the identification of critical facilities. Further, we believe Generator

Organization	Yes or No	Question 1 Comment
		Owners and Generator Operators may also be involved since critical facilities may not be just limited to transmission facilities of control centres. Large power plants, if deemed inoperable, can also result in wide-area reliability concerns. We suggest the SAR be revised to include these two entities as potential applicable entities.
American Electric Power	No	Please see comments provided in response to Question 4.
Hydro One	No	The SAR does not ask the SDT to identify timelines by which the third-party verification, following the completion of the risk assessment, would be required. The FERC Order also does not specify timelines for how soon the third-party verification must be completed after the completion of the risk assessment. The scope of the standard should be limited to protection against physical attacks.Identifying which physical facilities are critical facilities should be determined through a BPS assessment of risk and the methodology by which this assessment is conducted should be identified in the standard. The assessment of risk or vulnerabilities should consider other standards including CIP and the new GMD Stage 2 project which will be a new TPL standard.
American Transmission Company, LLC	No	Currently, only Transmission Owners (TOs) and Transmission Operators (TOPs) are applicable Reliability Functions checked on the SAR on page 4. ATC believes those having experience in performing risk assessments and identifying critical facilities should also be included, which would be Planning Coordinators(PCs), Reliability Coordinators(RCs), and Transmission Planners(TPs). (and checked as applicable in the SAR for Reliability Functions on pp. 3 and 4) The basis for making PCs, RCs, and TPs applicable to the SAR and new Standard is also implied by one of the FERC Directives below addressing the need for a risk assessment: The following is an excerpt from the FERC Order:..... the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk

Organization	Yes or No	Question 1 Comment
		assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System.5 Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards.6 Instead, the Commission is directing NERC to develop Reliability Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.In addition, ATC believes that Generator Owners (GOs) and Generator Operators (GOPs) should be added to the Reliability Functions of the SAR. The FERC Order states that "The proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities." To address owners and operators of generation facilities that are part of the Bulk-Power System, GOs and GOPs should be included in the Reliability Functions of the SAR. With the above justification, ATC is recommending that the GOs, GOPs, PCs, RCs and TPs be checked on the SAR as applicable Reliability Functions.
Utility Services, Inc	No	The SAR attempts to address the Commission's directive by requiring only Transmission Owners and Transmission Operators to protect certain types

Organization	Yes or No	Question 1 Comment
		of facilities , however this may not fully address the directives. The Commission is seeking to physically protect BPS facilities that will impact to the reliable operation of the BPS. Generation is recognized to be a part of maintaining the reliability and resiliency of the BPS. Based on several factors, including but not limited to location and operating profile, a significant generation facility could have a huge effect on the reliable operation of the BPS. The SAR should, at a minimum, examine whether generating stations consisting of 3000 MW or more need to be included in the applicability of this project. This matches up to the treatment of the other types of assets being contemplated herein.
Nebraska Public Power District	No	If a list of the most critical substations exists, why are we trying to develop a new process to determine the list without first getting to see the list? The draft standard is due to FERC within 90 days, but we are being asked to develop a process to match their list, when we don't even know what is on the list. Shouldn't Congress get involved and pass a law within 90 days to require the military to protect the substations? No, just as we shouldn't have to draft a new standard within 90 days. Our NERC standard development process, similar to the process Congress uses to pass new federal requirements is intentionally designed with checks and balances, plus adequate time for review to prevent knee-jerk reactions to events. We need to spend time to get this right and not rush something through.This expedited standard development has the potential to derail our entire NERC standard development process. I feel like we have been blind folded and put into a room and told to hit a small target with a dart and we don't even know which wall or direction to throw the dart. We work in a very complex industry with very talented staff across North America. FERC's staff is more appropriately aligned toward oversight, without the technical expertise to understand the full impact of implementation of new rules and regulations. Why are we jeopardizing our entire process for this standard? Is there an imminent threat? If so, our leaders should find a more

Organization	Yes or No	Question 1 Comment
		appropriate path for a solution (i.e., deploy our military). We already have multiple NERC requirements to identify and designate our facilities as critical. Introducing a new requirement to identify critical facilities will create confusion and unintended consequences. The CIP standards have been through several iterations of identifying critical facilities and continue to evolve. This has been a moving target, so why introduce yet another process to determine critical facilities. Our planning standards require us to study our systems and methodically improve the infrastructure to prevent cascading outages. Do those planning standards need to be modified to consider physical attacks? Would that be a more appropriate path to a solution for this issue?
Ameren	No	1) The related standards section of the SAR should include CIP-002-5 so that the criteria to determine which facilities are critical as a preliminary list for the new physical security standard will not conflict with the bright-line criteria in CIP-002-5.
Tri-State Generation and Transmission Association, Inc.	No	TSGT does not agree that Transmission Operators should be included in the Reliability Functions. The March 7, 2014 FERC Order, paragraph 1, states "...owners or operators of the Bulk-Power System, as appropriate...". Transmission Owners have the legal and/or contractual ability to dictate how physical environments within a facility are addressed. There is nothing within the TOP function that formally allows the entity to dictate or ensure that any physical security concerns are met under this standard, unless otherwise dictated by contracts and/or agreements. If Transmission Operators are kept as a Reliability Function under this standard, the standard should clearly define which TOPS versus TOs should be included to ensure the "appropriate" entity is included and that the same facilities are not repeatedly reported by multiple entities.

Organization	Yes or No	Question 1 Comment
Salt River Project	No	The SAR, under the section "Related Standards" lists only CIP-006-5, CIP-008-5 and CIP-009-5. It should also consider additional related standards CIP-002-5, CIP-002-3, CIP-006-3, CIP-008-3, CIP-009-3, EOP-004-1, and the TPL family of standards. The SAR should work both to avoid inconsistencies between any new standard and the existing standards and also avoid redundancies as well.
Kansas City Power & Light	No	The FERC order references facilities and it is assumed this is linked to the existing definition of Critical Assets as defined in the Glossary of Terms. This definition is scheduled to be retired on March 31, 2016. There are many references to critical in the standards. Clarity as well as consistency is needed in the definition of critical and expressly for what purpose (reliability, security, relisiency, etc.). If the definition of critical facilities will be retired, common understanding of this term should be defined somewhere for consistent language between ERO staff and registered entities. The distinction between critical facility and critical asset should also be defined. Also, FERC's interpretation of facility is inconsistent with the NERC definition of Facility as FERC implies a control center is a facility in Footnote 6 on Page 3 of the order. Before this would become mandatory and enforceable, resolution of definition of terms is required to ensure consistency in application.The SAR reference determines applicability only to the TO and TOP functions. Whether based on the registry criteria or functional model activities, the determination of critical can be impacted or influenced by Transmission Planners, Generator Owners and Generator Operators who also model, plan, own and operate facilities on the BES. Applicability should be considered for Balancing Authorities, Planning Coordinators, and Reliability Coordinators depending on criticality for the purpose of reliability, security and resiliency. While the SAR refers to the entire order being incorporated into the SAR, KCP&L recommends that the SDT specifically list each of the directives in the SAR such that the

Organization	Yes or No	Question 1 Comment
		stakeholders can be assured that they have all been included and will then be addressed by the SDT.
Northeast Power Coordinting Council	Yes	Agree generally with the scope. Care must be taken that the requirements developed are consistent with the applicable reliability functions as noted in the SAR. The scope of the standard should be limited to protection against physical attacks. The determination of which physical facilities to protect (identified to be "critical") should come through a BPS assessment of risk that will need to be defined in the Standard, and depending on how that is done, might involve other types of registered entities or work done under other standards (e.g., CIP or even the GMD Stage 2 effort in which a new TPL Standard is under development, for similar reasons of determining what system risks to address).Regarding the Applicability, the purpose of this project is develop a standard that will require owners and/or operators of the Bulk Power System, as appropriate, to identify facilities on the Bulk Power System that are critical to the reliable operation of the Bulk Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. Such tasks might require power system impact analyses not unlike the type required for system impact assessments, with a focus on losing all the facilities at a location (e.g. a transmission substation, a large power plant, a right of way, etc.). We do not disagree with the applicable entities as specified in the proposed SAR, but are looking for clarification on how the assessments are obtained, and whether other functional entities might be asked for input from owners/operators. Put another way, depending on the types of impacts the Standard will seek to protect against, entities within the entire Interconnection, or maybe even specific regions within the Interconnection, might need to be included in the Standard. Can NERC or the SDT provide guidance on whether the loss of generating facilities might have interconnection or area wide impacts that the Standard needs to

Organization	Yes or No	Question 1 Comment
		protect against happening?To avoid compromising operations as stated in the SAR, we believe that consideration should be given to entities focusing more on the resiliency and the redundancy of the network rather than on additional physical security measures. Attacks may not be able to be prevented, but the consequences of an attack can be mitigated. This is the type of assessment that is best performed using the techniques in the TPL standards.Furthermore, according to the SAR, the SDT is to develop a standard that addresses risk factors, levels of acceptable security and the implementation of a protection plan. We believe that these elements can not be standardized as threat assessments are not the same from one entity to another. Consequently, the acceptable levels of safety cannot be identical. All of these factors lead us to believe that the development of fixed criteria regarding levels of acceptable risk and security cannot be identical from one entity to another. The SDT also has to consider and address the standard with respect to Canadian differences.
Duke Energy	Yes	(1)Duke Energy agrees with the scope and contents of the SAR.
ISO RTO standards Review Committee	Yes	We generally agree with the purpose and scope of the SAR, but we ask for clarification on how the SAR will address certain aspects of the FERC Order. Based upon the FERC Order for Physical Security Standards, we understand the task for NERC and the industry is to develop a standard that will require owners and/or operators of the Bulkâ€Power System, as appropriate, to identify facilities on the Bulkâ€Power System that are critical to the reliable operation of the Bulkâ€Power System. Then, owners or operators of those identified critical facilities should develop, validate and implement plans to protect against physical attacks that may compromise the operability or recovery of such facilities. Such tasks may require power system analysis not unlike the type required for transmission planning assessment, with a focus on loss of all the facilities at a physical location (e.g. a transmission substation, a large power plant, a right of way, etc.). We

Organization	Yes or No	Question 1 Comment
		do not disagree with the applicable entities as denoted in the proposed SAR snd are not seeking to expand the SAR to apply to Planning Authority (PA) and Reliability Coordinator (RC). However, we ask for clarification of how the assessments are obtained. Depending on the nature of the type of risk assessment developed under this Standard, certain tasks may need to involve the PA and/or the RC. Moreover, while the identification of "critical facilities" might not be the same as what may be identified under CIP-002-5 effective April 1, 2016 for High and Medium impact systems), CIP-002-5 (or PRC-023) might provide a model to use for RC/PA providing information to asset owners. We ask if these requirements can and will be relied upon.
ACES Standards Collaborators	Yes	ACES supports Project 2014-04 Physical Security SAR and NERC's efforts to protect the BES from either a cyber or physical security attack. NERC guidance should be developed to provide industry with examples of acceptable protections against various threat vectors and what level of resiliency should be in place. We support the drafting team in its development of a consistent and effective physical security standard for impacted registered entities across the regions. We also caution the drafting team to consider and minimize unintended consequences of these standards. For example, if the standards require visual impairments to prevent a Metcalf style attack could such visual impairments become projectiles during a storm. If so, would such visual impairments improve reliability in areas prone to many storms and tornadoes?
Exelon	Yes	Yes, Exelon agrees the primary goal is to develop a standard with clear unambiguous requirements that address the FERC directives.
Occidental Energy Ventures Corp.	Yes	Occidental Energy Ventures Corp. ("OEVC") agrees that the SAR properly captures the language and intent of FERC's order to address physical attacks on the BES. In addition, it is appropriate to limit the scope to high priority transmission assets - which we believe pose the most difficult

Organization	Yes or No	Question 1 Comment
		logistical challenges based upon their sheer number and wide geographic distribution.Having said that, there is a concern that the 90 day turn around interval mandated by the Commission could introduce flaws that would normally be caught in the vetting process. We realize that FERC has the legal authority to compel an expedited time frame, but would prefer that the SAR clearly indicate a commitment to risk-based principles that will allow flexibility to the industry and CEA community alike. For example, it may be appropriate at this time to require entities to develop strategies that engage law enforcement and the FBI when a threat appears - whereas a requirement to fortify substations and/or control rooms would not be. As the industry gains experience with protective techniques through exercises and actual experience, the best-in-class strategies can be encoded in a standard - but not before.
Madison Gas and Electric Company	Yes	The SAR seems to directly reflect the FERC Order but to assure system reliability and perform adequate studies the PC and TP may need to be added to the applicability section, since they have the ability to perform reliability studies. Plus studies could be used within the TPL Standards.
OPG	Yes	The reliability functions identified in the SAR are TO (Transmission Owner) and TOP (Transmission Operator). GO (Generator Owner) and GOP (Generator Operator) are not identified and this makes good sense. BPS impacted equipment that may be owned by a GO is contained within a plant environment and are already protected by existing Physical Security Measures in place to protect the plant.
City of Austin dba Austin Energy	Yes	City of Austin dba Austin Energy (AE) agrees with the scope and contents of the SAR; however, we think it is appropriate to include #7 in the list of Applicable Reliability Principles. #7 states “The security of the

Organization	Yes or No	Question 1 Comment
		interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis."
Northeast Utilities	Yes	NU agrees with scope and applicability. NU urges the SDT to take care that the requirements developed are consistent with the applicable reliability functions (TO & TOP) as noted in the SAR.
FirstEnergy Corp.	Yes	
Peak Reliability	Yes	
Dominion	Yes	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	
Minnkota Power Cooperative	Yes	
Entergy Services, Inc.	Yes	
Encari	Yes	
Entergy Services, Inc.	Yes	
Idaho Power Co.	Yes	
Orlando Utilities Commission	Yes	

Organization	Yes or No	Question 1 Comment
LCRA Transmission Services Corporation	Yes	
Manitoba Hydro	Yes	

2. **Are you aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project? If yes, please identify the Regional Variance**

Organization	Yes or No	Question 2 Comment
FirstEnergy Corp.	No	
Peak Reliability	No	
Dominion	No	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	No	
Duke Energy	No	
Tennessee Valley Authority	No	
ISO RTO standards Review Committee	No	
ACES Standards Collaborators	No	
Bonneville Power Administration	No	

Organization	Yes or No	Question 2 Comment
Foundation for Resilient Societies	No	
Minnkota Power Cooperative	No	
Entergy Services, Inc.	No	
Self	No	
Encari	No	
Exelon	No	
Consumers Energy	No	
Entergy Services, Inc.	No	
Idaho Power Co.	No	
City of Tallahassee - Electric Utility	No	
Westar Energy	No	
Orlando Utilities Commission	No	
Occidental Energy Ventures Corp.	No	
LCRA Transmission Services Corporation	No	

Organization	Yes or No	Question 2 Comment
Colorado Springs Utilities	No	
City of Tallahassee	No	
City of Tallahassee	No	
Madison Gas and Electric Company	No	
Manitoba Hydro	No	
American Electric Power	No	American Electric Power is not currently aware of any regional variances associated with approved NERC Reliability Standards that will be needed as a result of this project.
OPG	No	
City of Austin dba Austin Energy	No	
Hydro One	No	
American Transmission Company, LLC	No	
Northeast Utilities	No	
Xcel Energy Inc.	No	
Utility Services, Inc	No	

Organization	Yes or No	Question 2 Comment
Ameren	No	
Tri-State Generation and Transmission Association, Inc.	No	
Salt River Project	No	
Northeast Power Coordinting Council	Yes	There are regional differences in Quebec. The SDT should not establish predefined criteria for risk assessment since it cannot be the same for different entities. Each entity should have its basis of a threat and security level defined accordingly.
SPP Standards Review Group	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.
The Empire District Electric Company	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.
the empire district electric company	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.
The Empire District Electric Company	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves. It may be necessary to give special consideration to specific situations.

Organization	Yes or No	Question 2 Comment
Kansas City Power & Light	Yes	Regional variances may need to be incorporated into the standards simply due to geographical differences across the regions which will need to be factored into the standards themselves - topography, climate, vegetation,etc.

3. Are you aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard(s)? If yes, please identify the jurisdiction and specific regulatory requirements.

Organization	Yes or No	Question 3 Comment
ISO RTO standards Review Committee	No	At this time, we are not aware of any jurisdictional issues that need to be considered by the drafting team and addressed in the standard. In addition, if the standard should involve protection of nuclear power plants, then there are differences in nuclear power plant regulations between the USA and Canada that may require recognition by the proposed standard.
American Electric Power	No	American Electric Power is not currently aware of any Canadian provincial or other regulatory requirements that may need to be considered during this project in order to develop a continent-wide approach to the standard.
Dominion	No	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	No	
Tennessee Valley Authority	No	
ACES Standards Collaborators	No	

Organization	Yes or No	Question 3 Comment
Bonneville Power Administration	No	
Foundation for Resilient Societies	No	
Minnkota Power Cooperative	No	
Entergy Services, Inc.	No	
Self	No	
Encari	No	
Exelon	No	
Consumers Energy	No	
Entergy Services, Inc.	No	
Idaho Power Co.	No	
City of Tallahassee - Electric Utility	No	
The Empire District Electric Company	No	
the empire district electric company	No	

Organization	Yes or No	Question 3 Comment
The Empire District Electric Company	No	
Orlando Utilities Commission	No	
Occidental Energy Ventures Corp.	No	
LCRA Transmission Services Corporation	No	
Colorado Springs Utilities	No	
City of Tallahassee	No	
City of Tallahassee	No	
Madison Gas and Electric Company	No	
Manitoba Hydro	No	
OPG	No	
City of Austin dba Austin Energy	No	
American Transmission Company, LLC	No	
Northeast Utilities	No	

Organization	Yes or No	Question 3 Comment
Xcel Energy Inc.	No	
Utility Services, Inc	No	
Ameren	No	
Tri-State Generation and Transmission Association, Inc.	No	
Salt River Project	No	
Kansas City Power & Light	No	
Northeast Power Coordinting Council	Yes	At this time, it is uncertain whether or not there are any jurisdictional issues that need to be considered by the Standard Drafting Team and addressed in the standard. It depends on the proposed requirements as they relate to detection, protection and reporting of potential physical risks to safeguard physical security. In addition, if the standard should involve protection of nuclear power plants, then there are differences in nuclear power plant regulations between the United States and Canada that may require recognition by the proposed standard.
Duke Energy	Yes	(1)The SDT should ensure that facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission are considered for exemption in the drafting of a Physical Security standard.
David Kiguel	Yes	Please see my comment with respect to confidential information above (Question 1).
Hydro One	Yes	As well, there may be provincial regulations in Ontario that require government-owned entities such as utilities to follow procurement rules and if the new standard included timelines by which assessments must be verified by third-party, these utilities may not be able to go through procurement processes for normal work (i.e.

Organization	Yes or No	Question 3 Comment
		not emergency or restoration work) quickly enough if the timelines are insufficient. (I am looking into this to confirm).

4. Are there any other concerns with this SAR?

Organization	Yes or No	Question 4 Comment
FirstEnergy Corp.	No	
Peak Reliability	No	
Dominion	No	
Southern Company; Southern Company Services,Inc; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	No	
Self	No	
Exelon	No	
Consumers Energy	No	
Entergy Services, Inc.	No	
City of Tallahassee - Electric Utility	No	
Orlando Utilities Commission	No	

Organization	Yes or No	Question 4 Comment
LCRA Transmission Services Corporation	No	
City of Tallahassee	No	
OPG	No	
City of Austin dba Austin Energy	No	
Northeast Power Coordinting Council	Yes	The Standard Drafting Team is urged to not be too prescriptive in the development of these requirements. Operators should be able to conduct a vulnerability assessment and implement any mitigation actions that were deemed appropriate by the entity. The Standard Drafting team should carefully consider the cost impact that the standard will have on entities to implement and therefore limit the site selection.Minimum vulnerabilities should be defined to be included in vulnerability assessments.Critical facilities determination are recommended to be carried out via a TPL standard based assessment.Timing should be provided for the effective date of standard versus the time required to conduct assessments and implement the mitigation actions identified.It has to be considered that electrical analysis and physical analysis are related, but are not one in the same. For example, using an electrical criteria, e.g., >3,000MVA, does not take into account that multiple voltages can reside on a single site, within a single footprint and fence. “Substations” is not a stand alone term. The SAR needs to recognize that there is not a total correlation between Cyber Security (CIPâ€002â€5.1) and Physical Security (CIPâ€014â€1). They are related, but different, and may need to use identical and as well as some different criteria. The current proposal for CIPâ€014 is to use the same criteria as those specifying a Medium Asset in CIPâ€002â€5.1. This may represent an over simplification. Physical Security is different. You do not need access in order to violate physical security. A TPL standards based assessment is a better approach.The SDT

Organization	Yes or No	Question 4 Comment
		must ensure that the scope of this standard and applicability of facilities subject to the standard is consistent with existing CIP standards.Furthermore, consider the impact of this standard on the existing standard EOP-004-2 and ensure the coordination with the EOP-004-2 standard.We believe that the SDT should consider network redundancy in the case of an attack, the potential consequences associated with a physical attack and threats specific to each entity before imposing a standard level of acceptance for all.The SDT should define how the verification of the risk assessment used by the owner or operator of critical facilities will be completed. The standard should identify the methodology by which critical facilities were identified. Once the methodology is determined, then the SAR should also define the methodology for doing this verification. The definition of the methodology for review should be applied to the review of all three of the identification of critical facilities, determination of threats and vulnerabilities, and mitigation plans, and that the standard should clarify whether the mitigation plans also have to be reviewed by a third party.The SDT should ensure that the new standard does not call for requirements that will impact or impede the normal operational capacity, access for maintenance or restoration, or the safety of people or equipment.The standard should clearly define the timelines for conducting assessments and implementing the mitigation actions identified with respect to when the standard becomes effective. Timelines for assessment of risk or vulnerabilities in this new standard should coincide with the timelines for which assessment of risk or vulnerabilities for other standards including the CIP and the new GMD Stage 2 project which will be a new TPL standard.
Duke Energy	Yes	(1)Duke Energy would like to reiterate to the SDT that any set of physical security standards need to provide the specific deliverables and that the requirements developed are clear and concise. We ask that the SDT proceed with caution and focus its attention on all potential physical threats and vulnerabilities to transmission substations, and not solely focus its attention on the recent activities in California and elsewhere. Also, stakeholders should have the flexibility to implement a staged level approach of security measures that are appropriate for the criticality of the facility

Organization	Yes or No	Question 4 Comment
		and the assessment of the vulnerabilities at a facility.(2)In addition to the CIP standards identified in the SAR for review of consistency in language and terminology, Duke Energy recommends the SDT review CIP-002-5 and EOP-004-2 as well.
Tennessee Valley Authority	Yes	While not stated in the SAR, it appears the SDT is preparing to develop an initial draft physical security standard as CIP-014-1 based on the ballot pool title. We agree that physical security of critical power system facilities can be considered a critical infrastructure protection issue; however we are concerned that development and implementation of a physical security standard (as outlined in the FERC order) under the CIP family of standards during the transition period from CIP version 3 to CIP version 5 will create an unnecessary distraction from the ongoing industry efforts to protect Cyber Assets under a changing regulatory framework. We respectfully request the SDT to consider developing the physical security standard for critical facilities (as outlined in the FERC order) under the FAC standards group to maintain a distinction from the CIP version 5 standards that are more focused on BES Cyber Assets and the associated protection of those Cyber Assets.
ISO RTO standards Review Committee	Yes	The IRC SRC is committed to working under this extremely expedited standards process timeline to provide our resources and technical expertise to help develop a standard that satisfies the FERC directive and above all, is effective and adds value to the numerous in effect reliability standards and practices that are designed to protect the Bulk-Power System from instability, uncontrolled separation and cascading failures. We do ask the standards drafting team to be aware that many facility owners already have physical protections in place for facilities they have determined to be critical. A NERC standard for physical security needs to be flexible so that it not only increases protections where they may be deficient - but also does not hinder or disincents the continued use of any protections already in place which have been effective.

Organization	Yes or No	Question 4 Comment
ACES Standards Collaborators	Yes	(1) FERC has stated in their order that they want grid owners and operators to "consider resilience of the grid" when identifying critical facilities. We recommend that the drafting team provide additional guidance to what level of resilience is needed, how will this be measured for each type of facility, and the level of resilience based upon risk to the BES. (2) FERC is requiring that an applicable entity must have "NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity" review the process for identifying a critical facility. Given that only a TO and TOP have been identified as potential applicable functions, we question if this directive has been considered appropriately in the SAR.(3) Given that third parties may evaluate critical facility information, further guidance is needed and controls are required to address this highly sensitive level information. Is this information subject to the Freedom of Information Act? This will need to be clear as to how information, data, and protection plans are to be reviewed, secured and monitored.Thank you for your time and consideration.
SPP Standards Review Group	Yes	The 90-day response requested by FERC is well short of the normal standard development time at NERC. This process is an established, ANSI accredited and transparent process which is intended to consider all technical considerations and to establish a broad stakeholder consensus. To drastically reduce the process to a 90-day turnaround will present a challenge to developing a broad industry consensus and achieving the best technical solution.If the apparent driver behind this effort, the Metcalf event referenced in the WSJ article, truly raises a credible threat to the reliability of the Bulk Electric System(BES), it should be addressed logically in a well, thought-out process to reach the right conclusion and not be done in haste. The credibility of the analysis referred to in the WSJ article, pointing to a limited set of substations in North America causing a widespread outage, must be vetted by industry experts to first determine if there is a reliability gap in existing NERC standards. This is an appropriate scientific and logical approach to establishing a benchmark for developing any additional standards to further protect the North American electric grid from harm.We request that in order to give this project the

Organization	Yes or No	Question 4 Comment
		proper thought and effort that it deserves, NERC should reconsider seeking an extension from FERC in order to allow more time for a broader cross section of industry and as many technical experts as possible to participate in developing a product which will be more effective at maintaining the reliability of the BES.What does RISC say about the need for this standard? Have they been consulted? Also, what about the Independent Expert Review Panel? Have these parties voiced an opinion?Do the studies referenced in Table 1 of the TPL standards point to the list of the limited set of substations which this project is intended to address? Are the substations tied to these studies in any manner?The order mentions facilities being inoperable or not available but there was no reference to misuse as there is in the CIPs standards. Can we assume that cyber-type attacks on substations are already adequately accounted for in the CIPs standards and therefore do not need to be factored into the Physical Security standard?
Bonneville Power Administration	Yes	BPA believes it is virtually impossible to fully protect all critical BES facilities from attack by a determined foe. The means to damage BES facilities is readily available, constructible, and implementable regardless of what level of physical hardening is implemented. There are many question and issues to resolve, and the 90 day drafting period may not be long enough to address them all. The biggest general question to answer is what will be considered adequate protection.Will we need a 24 hour on site armed security force because the location is too remote to augment detection technology with fast response that will minimize the scale of impact to an acceptable level of loss? Will we need security walls constructed to be as impervious as those of a maximum security prison? The list of potential risk mitigation barriers is endless, as is the cost of building and maintaining elaborate barriers for facilities that cover acres of ground. It will be interesting to see what a standard of this type will prescribe as required to obtain a level of risk that is significantly lower than the current state potential for experiencing another Metcalf type event.BPA has concerns that the compressed time frame will impact quality and thoroughness of the dialog needed to develop “unambiguous” standards.

Organization	Yes or No	Question 4 Comment
Foundation for Resilient Societies	Yes	Detectors for Intentional Electromagnetic Interference (IEMI) and Electromagnetic Pulse as a Physical Security MeasureBecause an IEMI attack would take place in the physical proximity of critical facilities of the bulk electric system, it should be considered a physical security vulnerability for standard-setting for FERC Order RD14-6-000, just as a kinetic attack or physical intrusion would be covered in a physical security standard. Electronic upsets and failures occur under normal operating circumstances, even in high-reliability equipment such as that supporting critical infrastructure. Intentional Electromagnetic Interference (IEMI) and other electromagnetic pulse (EMP) induced upsets and failures, however, are different from those encountered in the normal operation of infrastructure systems, and in fact have unique aspects not encountered under any other circumstances. A coordinated physical attack using IEMI could produce nearly simultaneous upset and damage of electronic equipment over wide geographic areas. Since such non-random upset and damage is not encountered in other circumstances, the normal experience of otherwise skilled system operators and others in positions of responsibility and authority will not prepare them to identify what has happened to the system, what actions to take to minimize further adverse consequences, and what actions must be carried out to restore the impacted systems as swiftly and effectively as possible.Special system capabilities and operator awareness, planning, training, and testing will be required to deal with IEMI/EMP-induced system impacts. The first requirement is for the operators of critical infrastructure systems to be able to determine that a IEMI/EMP attack has occurred.It will be necessary to distinguish high altitude nuclear EMP (HEMP) effects from localized IEMI effects that could be generated by a cruise missile or ground based vehicle employing non-nuclear intentional electronic interference devices. IEMI attacks have fast rise times measured in nanoseconds but limited geographic range; detectors can be designed to distinguish between nuclear EMP and IEMI.Indications of IEMI or EMP attack should be transmitted to electric grid control rooms so operators can gain a comprehensive picture and adjust operational response. Without electromagnetic sensors and

Organization	Yes or No	Question 4 Comment
		associated telemetry and alarm systems, operators would be flying blind in case of IEMI/EMP attack.
Minnkota Power Cooperative	Yes	a) On page 5 of the SAR, under the Related Standards section, there lists 3 CIP Reliability Standards (CIP-006-5, CIP008-5, and CIP-009-5), with an explanation to review them to ensure no language and terminology inconsistency with requirements developed under this project. CIP-011-1 - Cyber Security Information Protection should also be added to the list. Paragraph (10) of the FERC order describes the importance of guarding sensitive or confidential information. While CIP-011-1 is focused towards BES Cyber System Information, the information protection program entities may adopt could be hindered if CIP-011-1 was not considered when developing new standard(s) to address the directives in the March 7, 2014 FERC Order regarding the physical security of critical facilities on the Bulk-Power System.b) On page 3 of the SAR, under the Reliability Functions section, lists the Functions the Standard(s) would be applicable to (TO and TOP are checked). Shouldn't GO and GOP also be checked. The FERC order states the "proposed Reliability Standards should require owners or operators of the Bulk-Power System, as appropriate, to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System". The key words to note are "owners or operators". A generation plant, under the BES definition enforceable July 1, 2014, could be considered critical to the reliable operation of the Bulk-Power System.
Entergy Services, Inc.	Yes	Compressed timeline will limit NERC's ability to acquire input from owners or operators of the Bulk-Power System.
Encari	Yes	If the proposed standard under this project takes effect and is implemented prior to 3/31/2016, then the proposed standard should take into account CIP-002-3 which has a process for identifying Critical Assets. After 3/31/2016, CIP-002-3 and the term "Critical Asset" become inactive.

Organization	Yes or No	Question 4 Comment
Idaho Power Co.	Yes	Related Standards. CIP-002-5 is not mentioned and as one of the instructions is 'to identify facilities on the Bulk-Power System that are critical to the reliable operation of the Bulk-Power System' unless we are going with another set of criteria and labelling the facilities differently, this seems to be what CIP-002-5 does.
The Empire District Electric Company	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. How will the industry be able to adequately respond to the directive when the process we use isn't designed for such a quick development time? Trying to respond within a 90-day period while maintaining some resemblance of our existing process will be difficult indeed. The apparent driver behind this effort, the WSJ article, seems a bit misdirected. The Metcalf event occurred over a year ago, yet the standard has been mandated to be issued within 90 days. If the issue was that critical, why hasn't something been done sooner? And if this is a truly critical situation, we need to be sure to move logically in a well, thought-out process to reach the right conclusion rather than respond with a "knee-jerk" reaction to a newspaper article. How was the list of 9 substations in the WSJ article determined? What studies were ran to make this determination? What process was used to validate the study? What were the credentials of those conducting the study? Numerous questions like these come to mind regarding the credibility of the analysis behind the study upon which the article is founded. The WSJ article referred to entire interconnections going down due to the loss of 9 substations across 3 interconnections. Four substations are credited with being able to bring down the entire EI. This is doubtful. This study must be vetted by industry experts to first establish if a reliability gap exists.
the empire district electric company	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. How will the industry be able to adequately respond to the directive when the process we use isn't geared to such a

Organization	Yes or No	Question 4 Comment
		quick turn-around? Trying to respond within a 90-day period while maintaining some semblance of our existing process will be difficult indeed. It's literally like trying to hit a target that is hidden in the dark.The apparent driver behind this effort, the WSJ article, seems a bit misdirected. The Metcalf event occurred over a year ago, yet no action has been taken to date to address the situation. If the issue was that critical, why hasn't something been done sooner? And if this is a truly critical situation, we need to be sure to move logically in a well, thought-out process to reach the right conclusion rather than respond with a knee-jerk reaction to a newspaper article. How was the list of 9 substations in the WSJ article determined, what studies were ran to make this determination, what process was used to validate the study, what were the credentials of those conducting the study? Numerous questions like these come to mind regarding the credibility of the analysis behind the study upon which the article is founded. The WSJ article referred to entire interconnections going down due to the loss of 9 substations across 3 interconnections. Four substations are credited with being able to bring down the entire EI. This is doubtful. This study must be vetted by industry experts to first establish if a reliability gap exists.We request that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.What does RISC say about the need for this standard? Have they been consulted? Also, what about the Independent Expert Review Panel? Have these parties voiced an opinion?Do the studies referenced in Table 1 in the TPL standards point to the list of 'the 9 substations' mentioned? Are the substations tied to these studies in any manner?The order mentions facilities being inoperable or not available but there was no reference to misuse as there is in the CIPs standards. Can we assume that cyber-type attacks on substations are already adequately accounted for in the CIPs standards and therefore do not need to be factored into the Physical Security standard?

Organization	Yes or No	Question 4 Comment
The Empire District Electric Company	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. How will the industry be able to adequately respond to the directive when the process we use isn't geared to such a quick turn-around? Trying to respond within a 90-day period while maintaining some semblance of our existing process will be difficult indeed. It's literally like trying to hit a target that is hidden in the dark.The apparent driver behind this effort, the WSJ article, seems a bit misdirected. The Metcalf event occurred over a year ago, yet no action has been taken to date to address the situation. If the issue was that critical, why hasn't something been done sooner? And if this is a truly critical situation, we need to be sure to move logically in a well, thought-out process to reach the right conclusion rather than respond with a knee-jerk reaction to a newspaper article. How was the list of 9 substations in the WSJ article determined, what studies were ran to make this determination, what process was used to validate the study, what were the credentials of those conducting the study? Numerous questions like these come to mind regarding the credibility of the analysis behind the study upon which the article is founded. The WSJ article referred to entire interconnections going down due to the loss of 9 substations across 3 interconnections. Four substations are credited with being able to bring down the entire EI. This is doubtful. This study must be vetted by industry experts to first establish if a reliability gap exists.We request that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.What does RISC say about the need for this standard? Have they been consulted? Also, what about the Independent Expert Review Panel? Have these parties voiced an opinion?Do the studies referenced in Table 1 in the TPL standards point to the list of 'the 9 substations' mentioned? Are the substations tied to these studies in any manner?The order mentions facilities being inoperable or not available but there was no reference to misuse as there is in the CIPs standards. Can we assume that cyber-type attacks on

Organization	Yes or No	Question 4 Comment
		substations are already adequately accounted for in the CIPs standards and therefore do not need to be factored into the Physical Security standard?
Westar Energy	Yes	The FERC imposed development timeframe of 90 days is inadequate. The normal Standard Development Process allows for a transparent process which incorporates stakeholder consensus.The quality of the regulation will be adversely impacted by such an accelerated schedule.Westar requests that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.
Occidental Energy Ventures Corp.	Yes	This project is one of several which FERC has clearly established their expectation of urgent action. The CIP Version 5 Cyber Security, Geomagnetic Disturbance, and Gas/Electricity Industry Interoperability standards come immediately to mind. In OEVC's view, this means that NERC's standards development prioritization must be updated to take on the new work load - even if other project activity needs to be suspended in favor of Project 2014-04.Furthermore, there are a large number of new and/or modified standards which are scheduled to take effect this year and next - Generator Validations, and Protection System maintenance are among the most pressing. As a result, OEVC believes it is time for a second iteration of the Paragraph 81 process to aggressively retire those requirements that do little to support BES reliability. We understand that the obvious candidates have been addressed, but the industry's efforts must be continually re-focused on higher-priority activities. As long as less urgent requirements remain on the books, we all must set aside resources to capture evidence of compliance to routine tasks; leaving fewer available to address far more important threats to the BES.
Colorado Springs Utilities	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process which incorporates stakeholder consensus. The result of this accelerated process will

Organization	Yes or No	Question 4 Comment
		be an inferior standard.We request that in order to give this project the proper thought and effort that it deserves, NERC seek an extension from FERC which will allow more time to complete the project. Allowing more time and consideration will result in a better product which will be more effective at maintaining the reliability of the BES.We feel the focus should be on recovery from an attack, not solely prevention. We believe this has a larger impact on the reliability of the BES. Include something in the new standard that BES information should be protected, especially for public entities subject to Open Records Acts.
Manitoba Hydro	Yes	(1) Related Standards to avoid inconsistencies should include CIP-004-5 which addresses physical access management, a component of overall physical security. (2) "Applicability" should include an RC or PA/PC, as these would be the most appropriate Reliability Functions to determine if the loss of a facility would result in instability etc.
American Electric Power	Yes	While American Electric Power (AEP) appreciates the need for expediency in this FERC docket and relevant NERC SARs/Standards, we caution against an assumption that because a specific category of threat may be perceived as new, no efforts are yet underway to protect against that threat. In reality, AEP already has in place significant protections to secure the reliability of the grid - as does most of the electric utility industry. Many of these protections are in system configuration and design, inherently minimizing the criticality of any particular transformer, transmission circuit or station. These system configuration and design protections are incorporated to foster transmission system reliability in the event of weather and/or normal equipment failures. But they also answer the need for protection from other physical threats. In many cases our existing safeguards will protect the grid against new threats, including intentionally created damage.AEP agrees with FERC Commissioner John Norris' concurring comments filed with RD14-6-000 on March 7: "The owners and operators of our Bulk-Power System have already taken significant steps to protect critical facilities from physical attack. NERC's standards development process will benefit from the lessons learned from the owners and operators of the Bulk-

Organization	Yes or No	Question 4 Comment
		Power System and the communication that will take place across the stakeholder community regarding physical security. However, I am concerned that the procedural approach chosen by the Commission will inappropriately preclude an open and transparent process in which all interested parties would be able to engage with the Commission as the standards development process gets underway."AEP does not fully understand NERC's SAR which describes this effort as a New Standard, but not an Urgent Action. Certainly, the uniquely short timeframes allowed first by FERC and then by NERC for stakeholder participation imply an element of urgency. With no provision for comment to FERC and reduced input ability at NERC, the industry and our customers run the risk of unnecessary costs resulting from rushed decisions made with inadequate data. Likewise, addressing only Transmission Owners and Transmission Operators will provide less than a complete picture. Reliability Coordinators and Balancing Authorities also have a role to play and excluding that role from consideration will yield sub-par results. Additionally, some of the issues covered in the SAR and the FERC docket seem to overlap with existing Standards. Violations of a Standard that could stem from this effort might also be violations of CIP-002, CIP-006, CIP-008 and/or CIP-009. Care must be taken to ensure that the Standards dovetail, rather than duplicate each other, which would create a double-jeopardy situation for grid owners.In addition to our concerns about the process, AEP has reservations about the substance of the proposed SAR as well. First, AEP questions how the SAR proposes to define critical facilities. FERC and NERC have implied that the number of critical facilities identified in this process will be relatively small - fewer than 100 of the 55,000 transmission stations dispersed throughout the country. However, for previous "critical asset" determinations requested by NERC, AEP has already identified almost that many just on our own system. This would indicate we are starting over with the definition of critical facilities, which is counter-intuitive if not counter-productive. CIP-V5 switches the focus from protecting discrete cyber assets to protecting systems. Shouldn't we consider this same approach for physical security? AEP suggests that we begin by determining how critical facilities will be defined: 1) Will it be a bright-line test or a triage approach? 2) What will

Organization	Yes or No	Question 4 Comment
		distinguish critical cyber facilities from physical, and will one facility category be deemed more critical than the other? 3) Is there a distinction between a “critical facility” and “critical assets” defined in previous initiatives?4) Will there be distinctions between staffed and unstaffed stations, control centers or shared facilities?AEP believes that critical physical facilities will largely be a subset of the critical cyber asset list, tempered by:1) Availability of equipment spares, 2) Equipment redundancy located at the same vs. adjacent stations, 3) Level of interconnection to other stations at a particular voltage level,4) Proximity to a nuclear station, 5) Availability of alternative black start paths, 6) A sundry list of similar considerations. This analysis suggests that determination of a particular station as a critical physical facility is not a yes/no question, but rather a tiered approach to physical criticality is required. Considering the above, two stations similarly configured but in different parts of the system may not have the same physical criticality. Therefore, AEP is pleased with the nod to regional differences and the flexibility indicated in RD14-6-000. However, the changes NERC and FERC are proposing could result in massive changes, bringing excessive additional costs with no guarantee of desired outcomes. The question then becomes whether the cost to the nation’s electric customers far outweighs the benefits from additional protections layered on top of existing protocols. Are we being overly reactive to the isolated case of the Metcalf Station attack in San Jose a year ago? Are we painting targets on our critical infrastructure? Even with increased physical security, there will always be some potential for an attack on a critical facility. Larger fences and armed guards will make attacks marginally more difficult. They will not make the facilities immune to attack. A second primary concern is cost recovery - an issue that neither FERC nor NERC has addressed. Should NERC determine that a bright-line definition of critical facilities is the best way to go, cost recovery would be easier for grid owners, but costlier for customers. If NERC gives grid owners discretion to identify their critical facilities through risk-based assessments and determine their own protection strategies, state regulatory commissions will question every decision made, creating regulatory lag. That said, a risk-based assessment resulting in tiered levels of

Organization	Yes or No	Question 4 Comment
		criticality would yield the strongest results from a grid protection standpoint. While grid protection is paramount, we must weigh options. Poorly executed, these Standards could carry astronomical real costs as well as opportunity costs. Meanwhile, many customers are about to bear significant cost increases based on changes required by the EPA's Mercury and Toxics Standards. While we need to make whatever investment is necessary to adequately protect the grid, we also need to be responsible stewards of the grid and our ratepayers' pocket books. We must make sure we have taken necessary steps as cost-effectively as possible and that we are not simply being reactionary.In summary, AEP supports:1) Risk-based assessments conducted by transmission owners to define their own critical facilities2) Triage protocols based on those risk-based assessments3) Acknowledgement and inclusion of existing protections4) Adoption of a CIP-V5 approach of protecting critical systems rather than discrete facilities5) Cost-based assessments that include opportunity costs and factor in cost recovery.
Hydro One	Yes	The SAR should ask the SDT to define how the verification of the risk assessment used by the owner or operator of critical facilities will be completed. The standard should identify the methodology by which critical facilities were identified? If it is the methodology, then the SAR should also define the methodology for doing this verification. The FERC Order states "the Reliability Standards should require that the identification of the criticalfacilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness." The definition of the methodology for review should be applied to the review of all 3 of identification of critical facilities, determination of threats and vulnerabilities, and mitigation plans, and that the standard should clarify whether the mitigation plans also have to be reviewed by a third party.There is risk that significant investments may be needed as a result of the new standard.There SDT should ensure that the new standard does not call for requirements that will impact or impede the normal operational capacity, access for maintenance or restoration, or the safety of people or equipment.Minimum vulnerabilities should be defined in the standard to be included in vulnerability

Organization	Yes or No	Question 4 Comment
		assessments.The assessment of critical facilities should be defined in a TPL standard based assessment.The standard should clearly define the timelines for conducting assessments and implementing the mitigation actions identified with respect to when the standard becomes effective.Timelines for assessment of risk or vulnerabilities in this new standard should coincide with the timelines for which assessment of risk or vulnerabilities for other standards including the CIP and the new GMD Stage 2 project which will be a new TPL standard.
Northeast Utilities	Yes	NU urges that the SDT not be too prescriptive in the development of these requirements. Entities should be able to conduct a vulnerability assessment and implement any mitigation actions that they deem appropriate. SDT should carefully consider the cost impact that the standard will have on entities to implement and therefore limit the site selection.SDT should define minimum vulnerabilities to be included in vulnerability assessments.SDT to provide for timing of the effective date of standard versus the time required to conduct assessments and implement mitigation actions identified.SDT should clearly limit the scope of the standard to protection against physical attacks.
Xcel Energy Inc.	Yes	A review of the CIP standards (Version 5) is required by the SAR. However, considering that many, if not all of the facilities in scope of this new standard will also likely be considered Critical Assets, as defined by CIP-002-5, this has the possibility of creating double jeopardy situations and added Regulatory oversight. Instead, please consider addressing physical security through an existing standard like CIP-006-5 or EOP-004-2 (Event Reporting).
Utility Services, Inc	Yes	The identification method that will be used to determine applicability to the standard is a concern. The drafting team should take care to respect the work already crafted by the previous CIP drafting teams in creating a format and brightline thresholds to identify those facilities that require protection. From historical experience we have seen that “Risk Assessment” style applicability is not consistently and uniformly

Organization	Yes or No	Question 4 Comment
		applied and should therefore be avoided. We have seen this causes major issues and we should not repeat past mistakes.
Nebraska Public Power District	Yes	If we truly have a small subset of nine key substations that are as critical as was quoted in the Wall Street Journal, why isn't the military protecting these substations? We use our military to protect our Air Force bases, Army forts, Naval yards, etc. Is this threat real or is it political sensationalism? Is the number of substations nine, or is it 30 or is it less than 100 as the Wall Street Journal quoted former FERC chairperson Wellinghoff. Shouldn't the electric industry experts be allowed to review the modeling for this analysis? Was the modeling in sufficient detail or were many networks equivalized? Was it a steady-state model or were dynamics evaluated? What was the experience level of the engineers doing the analysis (have they performed similar analysis at large utilities)? Should we revoke this SAR and replace it with another new standard that would restrict utilities from building any new substations above a certain level? Should the standard require planned additions/expansions to provide for redundancy and resiliency as the Department of Homeland Security and Department of Energy recently recommended in their Physical Security of Substations Briefing? Do we have to build 500 kV and 765 kV systems? Does the market save us any money to transfer power between regions, if we have to add these systems that open up vulnerabilities to physical attacks?Should Congress fund a US based manufacturing plant for transformers?Should North America (those within NERC) standardize voltage levels, so replacement transformers are more readily available?The list of philosophical questions can continue, but we are not ready to draft a standard on this issue without first debating the problem we are trying to solve. What is the problem we are trying to solve?The Wall Street Journal article implied we need to protect our substations from automatic weapons. Is this the problem we are trying to solve? Will we be required to build walls around our substations? What do we do about a substation that is located in a valley with unlimited firing angles from surrounding higher ground? How do we protect the miles and miles of transmission structures leading to these substations? Do we have to protect one substation away, two substations away, etc.By installing additional

Organization	Yes or No	Question 4 Comment
		security on these facilities, aren't we painting those assets as targets by clearly identifying them?
Ameren	Yes	1) The time frame that is outlined in this SAR to create a new physical security standard is very short and we are concerned that a cost effective, reasonable, workable standard cannot be drafted in this short amount of time. We understand the need for a new physical security standard but creating a standard this quick could result in an incorrectly written standard which will not be understood by industry. We are concerned that this does not solve the problem but will end up making a new one.
New Brunswick Power Corporation	Yes	It is our desire to ensure the SDT consider the impacts of physical security threats that can arise between entities (wide area view) rather than a strict focus on the effects of physical security risks on elements within a given entity's footprint. Taking this approach and allowing the entity to determine the specific impact criteria for their footprint, should align the violation risk factors and severity levels to account for higher level threats rather than burden the entities with lower impact concerns.
Tri-State Generation and Transmission Association, Inc.	Yes	In agreement with the Commissioner, John Norris's, concurrence, the uniquely expedited nature of this standard development procedural approach will preclude an open and transparent process, limit the engagement of the industry, and, without the time to properly vet the security risks and measures, will negatively impact reliability and consumer costs.Co-owned facilities are not addressed in the standard. Co-owned facilities will have multiple assessments by different entities. This will lead to different threat assessments and different physical security plans. Conflicts may and most likely will occur on co-owned facilities. This is something that must to be taken into consideration.There is no requirement for 3rd party verification for CIP-002-5.1 R2 which requires assessment and categorization of assets. 3rd party verification is not required there and should not be required here. Senior approval should be all that's necessary. Some possibilities to address the FERC order for verification of entities' plans include a submittal to the RC/RE upon their request as currently

Organization	Yes or No	Question 4 Comment
		required by many of the emergency operations plans or an annual submittal to the RC/RE.Something else to consider is that audits for TO/TOPs are on a 3 year cycle. The RE could review the assessments and plans during audits removing the requirement for 3rd party verification.Physical threats run the gamut of simple to highly complex. What will limit this review? Addressing ALL potential threats will be cost prohibitiveThe value necessary for a facility to qualify should be raised. The criteria from CIP-002 v5 is meant to include a larger portion of the grid. This criteria will include too many facilities which was not the intent of FERC.
Salt River Project	Yes	The SAR should closely follow the FERC Order that owners and operators are to develop their specific plans to protect against physical attacks that may compromise their facilities. The FERC Order provides for flexibility for owners and operators to determine the methodology they will use in identifying their critical facilities. The standard should direct the entities to focus on station facilities and not 'outside the fence' assets. Critical facilities vary widely both in the type and extent of potential vulnerabilities to physical attacks. Customized defenses and protections are esstential and the owners and operators are correctly given flexibility both in identifying which assets are critical and then developing the most appropriate plans for protection. That plan should not be primarily directed at physical deterrence of the threats, there are two other important facets of a security plan: operational security, and recovery after an event. The flexibility will help avoid potential conflicts between any new standards and existing ones. The objectives of the SAR are to provide clear, unambiguous requirements and standard(s) to address the FERC Order. This should not mean development of requirements with highly prescriptive, detailed and specific physical protection structures, activities and programs but instead should mean the SAR will develop clear direction on identification of critical facilities and credible physical threats to such facilities followed by prudent plans for protection that are appropriate for each such facility.
Kansas City Power & Light	Yes	The 90-day response requested by FERC is well outside the normal standard development process at NERC. This process is an established, transparent process

Organization	Yes or No	Question 4 Comment
		which incorporates stakeholder consensus. Trying to respond within a 90-day period while giving the appropriate diligence and consideration to the topic of protection of BES assets will be difficult. We recommend taking appropriate time to give this project the proper thought and effort that it deserves for diligent actions to be taken to protect the grid. We respectfully ask NERC to remain open to the potential need to seek an extension from FERC to allow more time to complete the project if deemed necessary. The order mentions facilities being inoperable or not available but there was no reference to misuse or a resiliency concept. We believe the SDT should consider these options including the concept of a capability / maturity model and on a continuum for improvements in the hardening of our BES facilities. Ultimately the goal is to focus on protection and security of assets.

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the Standard Drafting Team (SDT) for Project 2014-04 Physical Security were solicited March 13-18, 2014, and the SDT was appointed by the Standards Committee on March 21, 2014.
2. Technical Conference was held April 1, 2014.

Description of Current Draft

This is the first draft of the proposed Reliability Standard, and it is being posted for stakeholder comment and initial ballot. This draft includes proposed requirements to meet the directives issued in the FERC order issued March 7, 2014, in Docket No. RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Anticipated Actions	Anticipated Date
15-day Formal Comment Period with a 5-day Initial Ballot, pursuant to a Standards Committee authorized waiver.	April 10, 2014
10-day Formal Comment Period with a 5-day Additional Ballot (if necessary), pursuant to a Standards Committee authorized waiver.	May 2014
5-day Final Ballot, pursuant to a Standards Committee authorized waiver.	May 2014
BOT Adoption.	May 2014
File with applicable Regulatory Authorities.	No later than June 5, 2014

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Effective Date	New

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-1

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns any of the following:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection

Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities within the scope of a security plan approved by the Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1.

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in

widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated verifying entity shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated verifying entity.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3.

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 and verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

R4. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating implementation of the physical security plan.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

R6. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

6.1.1. An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.

6.1.2. An entity or organization approved by the ERO.

6.1.3. A governmental agency with physical security expertise.

6.1.4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated reviewing entity recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated reviewing entity.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the reviewing entity throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

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 during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three 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, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but less than or equal to	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but less than or equal to	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to 120 calendar days	The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days following

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			100 calendar days following completion of Requirement R1; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under R1 as required by part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	110 calendar days following completion of Requirement R1; Or The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under R1 as required by part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	following completion of Requirement R1; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under R1 as required by part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but failed to modify or document the technical basis for not	completion of Requirement R1; OR The Transmission Owner failed to have a third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had a third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					modifying its identification under R1 as required by part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 11	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control center identified in Requirement R1; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1.
R4	**Operations Planning,**	**Medium**	N/A	The Responsible Entity conducted an	The Responsible Entity conducted an	The Responsible Entity failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
	Long-term Planning			evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR The Responsible Entity failed to develop and implement a documented physical security

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include one of Parts 5.1 through 5.4 in the plan.	Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include two of Parts 5.1 through 5.4 in the plan.	Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include three of Parts 5.1 through 5.4 in the plan.	plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had a third party review the	The Responsible Entity had a third party review the	The Responsible Entity had a third party review the evaluation	The Responsible Entity failed to have a third party review

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion	evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days	performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review;	the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			of the third party review.	following completion of the third party review.	OR The Responsible Entity had a third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not and modify or document the reason for not modifying the security plan(s) as specified in Part 6.3.	failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 Applicability

The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners (TO) that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each TO that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many TOs that meet the applicability of this standard will not actually identify any such Facilities. Only those TOs with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators (TOP). A TOP's obligations under the standard, however, are only triggered if the TOP is notified by an applicable TO under Requirement R3 that the TOP operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only TOPs who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6.

The drafting team considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis

to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, the transmission analysis or analyses conducted under Requirement R1 will take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities.

Requirement R1

In performing the risk assessment under Requirement R1, the Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The following is guidance on how a Transmission Owner may perform a traditional power flow and stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a wide area. Using engineering judgment, the Transmission Owner should develop criteria to identify a contingency resulting in potential widespread instability, uncontrolled separation or Cascading within an Interconnection. For example, the criteria could include post-contingency

facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available remedial action schemes (RAS) or special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation.

Periodicity

A TO who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system.

TOs who have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment method, which may include, for example, consideration of factors such as the following system performance criteria:
    a. Thermal overloads beyond facility emergency ratings;
    b. Voltage deviation exceeding ± 10%,

c. Cascading outage/Voltage collapse,

d. Frequency below under-frequency load shed points.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or reviewing entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently.

Characteristics to consider in selecting a reviewing entity could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the transmission owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the TO's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk

assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the assessment conducted in Requirement R4.*

While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and EMS.

- *A timeline for implementing physical security resiliency or security measures specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security measures in their security plan according to risk, resources, or other factors.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Requirement R6

This requirement specifies review by an entity other than the TO or TOP with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected reviewing entity cannot be a corporate affiliate (*i.e.,* the reviewing entity cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A reviewing entity also cannot be a division of the Transmission Operator that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the drafting team believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP

certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

A third party that contributes to the threat assessment and development of the security plan may also serve as the reviewer. As with Requirement R2, the Responsible Entity has the flexibility to work with the reviewing entity throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a TO or TOP could coordinate with their unaffiliated reviewing entity to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) concurrently with review to satisfy Requirements R4 through R6 simultaneously.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Project 2014-04

April 9, 2014

Approvals Requested
CIP-014-1 Physical Security

Prerequisite Approvals
None

Effective Date

New or Revised Standards
CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Standards for Retirement
None

Initial Performance of Periodic Requirements
The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard. Subsequent risk assessments shall be performed according to the timelines specified in CIP-014-1, Requirement R1.

The initial performance of CIP-014-1, Requirements R2 through R6, must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows:

- Requirement R2 shall be completed as follows:
    - Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard.
    - Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2.

- Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.
- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2.
- Requirement R6 shall be completed as follows:
    - Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5.
    - Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project Overview for Project 2014-04 Physical Security

April 9, 2014

At a Glance: The Top Items to Know about Proposed Reliability Standard CIP-014-1

- Proposed CIP-014-1 Physical Security is drafted pursuant to the framework directed by the March 7, 2014, FERC order[1] directing a Physical Security Standard be filed by June 5, 2014. Consistent with the order, proposed CIP-014-1 includes a risk assessment (transmission analysis) for identification of critical facilities (as describe by FERC), evaluation of physical threats, and development of a physical security plan – with the assessment verified by a third party and the evaluation/plan reviewed by a third party.
    - The framework includes only those Transmission stations and Transmission substations (and associated primary control centers) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.
    - NERC will not request an extension of time to file the Standard, which is supported by the leadership of the Standards Committee (SC) and the Standards Drafting Team (SDT).
- Only a relatively small number of Transmission Owners and Transmission Operators will need to comply with the entire Standard.
    - Generator Operators and Generator Owners are not included as applicable entities.
    - Loss of generation connected to an applicable Transmission station or Transmission substation is considered in the risk assessment conducted by the Transmission Owners.
- The draft Standard was vetted at the April 1, 2014, NERC-sponsored technical conference and during the SDT meetings later that same week.
- The SC has approved a waiver to shorten the initial comment period to 15 days and the ballot period to the last five days of the comment period.
- There will be webinars to explain the Physical Security Standard on April 15 and April 17, 2014.
- **Your vote counts!** If you have registered in the ballot body, we need you to vote, and you must vote by the close of business on April 24, 2014. If you do not vote and quorum is not met on April 24, 2014, this will negatively impact the ability of the SDT to expeditiously move forward.
- Please review the FERC order, the draft Standard and associated guidance, the FAQ, and the RSAW posted on the 2014-04 project page. If you have any questions, please contact Stephen Crutchfield via email or by telephone at stephen.crutchfield@nerc.net or 609-651-9455 as soon as possible.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Frequently Asked Questions
Project 2014-04 Physical Security and Draft Standard CIP-014-1

April 9, 2014

1. Why are NERC and the Standards Committee pursuing a Physical Security Reliability Standard?

On March 7, 2014, the Federal Energy Regulatory Commission (FERC or Commission) issued an order directing NERC to file one or more Reliability Standards addressing physical security of certain critical facilities by June 5, 2014.[1] The Commission stated that the physical security Reliability Standard(s) should require entities to take a least the following three steps: (1) perform a risk assessment of their systems to identify their facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System; (2) evaluate the potential threats and vulnerabilities to those identified facilities; and (3) develop and implement a security plan designed to protect against physical attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Commission stated the Reliability standard(s) should also: (i) include a procedure that will ensure confidential treatment of sensitive or confidential information; (ii) include a procedure for a third party to verify the list of identified facilities and review the threat evaluation and security plan(s); and (iii) require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness.

In terms of the scope of the standard, FERC stated:

> . . . we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

NERC, the NERC Standards Committee (SC), and the Project 2014-04 Physical Security Standard Drafting Team (SDT) have been working diligently, with the assistance of stakeholders through an April 1, 2014, technical conference and SDT meetings, to draft a Reliability Standard that addresses all of the directives issued by FERC in the March 7, 2014, order. Proposed Reliability Standard CIP-014-1 is consistent with the scope of the Commission order and satisfies each directive described above.

NERC does not intend to request an extension of time for filing the proposed Reliability Standard and is committed to meeting the June 5, 2014, filing deadline. The SC and SDT leadership support this decision because they believe the framework in the FERC order is sufficiently clear to develop and file a Reliability Standard by the June 5, 2014, deadline.

2. Why does the proposed Reliability Standard's applicability section start with Transmission stations and Transmission substations identified under the medium impact criteria in CIP-002-5.1?

The SDT developed a technical guidance document appended to the end of CIP-014-1 that explains the applicability section and the requirements of the Reliability Standard in more detail.

In brief, the SDT concluded that FERC's March 7 order is reasonably understood to focus on the most critical Transmission facilities and determined that the CIP-002-5.1 bright line medium impact criteria for Transmission stations and Transmission substations was the appropriate place to start. The CIP-002-5.1 bright line medium impact criteria has been vetted with stakeholders, NERC, and FERC, and provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment under proposed Reliability Standard CIP-014-1. The SDT considered and rejected higher bright line thresholds because the SDT determined that higher bright lines could not be technically justified and may inadvertently exclude Transmission Owners that could have Transmission stations and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

The SDT understands that many of the Transmission Owners that have Transmission stations and Transmission substations that meet CIP-002-5.1's medium impact criteria are unlikely to have a Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To that end, if a Transmission Owner's risk assessment does not identify any such Transmission stations or Transmission substations and that risk assessment has been verified by a third party, the Transmission Owner has no further obligations under the proposed Reliability Standard, except to conduct subsequent risk assessments every five years to confirm that it continues to have no such facilities.

The SDT estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In turn, only a small number of Transmission Owners will actually have performance obligations under the entire proposed Reliability Standard. While the applicability section may include additional Transmission Owners subject to Requirements R1 and R2 only, the SDT found that the slightly broader applicability is necessary given the FERC directives, the inability to technically justify a higher bright line, and the importance of being conservative on applicability given the nature of the Reliability Standard's important topic.

The SDT also does not believe more study or time will justify another or higher bright line, given the diversity of Transmission Owners and the highly confidential nature of information related to the applicable Transmission stations and Transmission substations.

3. Why were Generator Operators and Generator Owners not included?

The SDT considered whether to include Generator Operators and Generator Owners in the proposed Reliability Standard and decided not to include them as applicable entities. First, the FERC order does not explicitly mention generation assets, and the order is reasonably understood to focus on the most critical Transmission Facilities. Second, the proposed Reliability Standard accounts for the loss of generation resources. A determination of whether a Transmission station or Transmission substation that meets CIP-002-5.1's medium impact criteria could, if rendered inoperable or damaged, result in widespread instability, uncontrolled separation, or Cascading within an Interconnection must consider the impact of the loss of generation. Specifically, the transmission analysis or analyses conducted under Requirement R1 will take into account the impact of the loss of generation. As such it is not necessary to include Generator Operators and Generator Owners to ensure that the impact of loss of generation is considered.

4. Why are only those primary control centers that have operational control of a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2 included in the proposed Reliability Standard? And what does "has operational control" mean?

The FERC order in footnote 6 specifically mentions control centers as a type of critical facility to be subject to the physical security Reliability Standard. Consistent with the order, the SDT found that it is important to include in the proposed Reliability Standard those primary control centers that have operational control over Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Specifically, the SDT concluded that in order to fully protect the Transmission stations and Transmission substations from causing

widespread instability, uncontrolled separation, or Cascading within an Interconnection as a result of a physical attack, it was imperative that these primary control centers be subject to the threat evaluation and development/implementation of physical security plans similar to the Transmission station(s) and Transmission substation(s) they operationally control.

There are two scenarios that the Standard recognizes related to identified primary control centers. In the first scenario, the registered Transmission Owner of the identified and verified Transmission station or Transmission substation is also the entity that operates the primary control center. In scenario two, the registered Transmission Owner is not the same registered entity that operates the primary control center. In this latter instance, the Transmission Operator would be the entity that operates the primary control center that has operational control of the Transmission Owner's identified and verified Transmission station or Transmission substation. Under scenario two, formal notice is required to the Transmission Operator, and that is covered in Requirement R3.

The phrase "has operational control" is specifically used to exclude from the Standard control centers that have no physical control over Transmission stations and Transmission substations, but only have the capability to monitor Transmission stations and Transmission substations, such as is the case with many, if not all, Regional Transmission Organizations and Independent System Operators. In other words, to have a primary control center in the scope of this Reliability Standard, the primary control center must have the ability to take electronic actions that can cause direct physical actions at the identified and verified Transmission station and Transmission substation, such as opening a breaker.

5. Why are unaffiliated third party verifications (of Transmission station and Transmission substation identification under Requirement R1) and unaffiliated third party reviews (of the evaluations under Requirement R4 and the security plans under Requirement R5) required in the proposed Reliability Standard?

The FERC order requires that the risk assessment be verified by an entity other than the owner or operator, and, similarly that the evaluation of threats and physical security plan be reviewed by someone other than the owner or operator. The order used the term "verify" in the context of identification of facilities and the term "review" in the context of physical threat evaluations and security plans. Therefore, the SDT decided to also use those terms in similar contexts in the proposed Reliability Standard.

a. What does unaffiliated mean?

The term unaffiliated means that the selected verifying and reviewing entities cannot be a corporate affiliate (*i.e.,* the verifying or reviewing entity cannot be an entity that corporately controls, is controlled by, or is under common control with, the Transmission Owner or

Transmission Operator). The verifying and reviewing entities also cannot be a division of the Transmission Owner or Transmission Operator (only applicable for the reviewer) that operates as a functional unit.

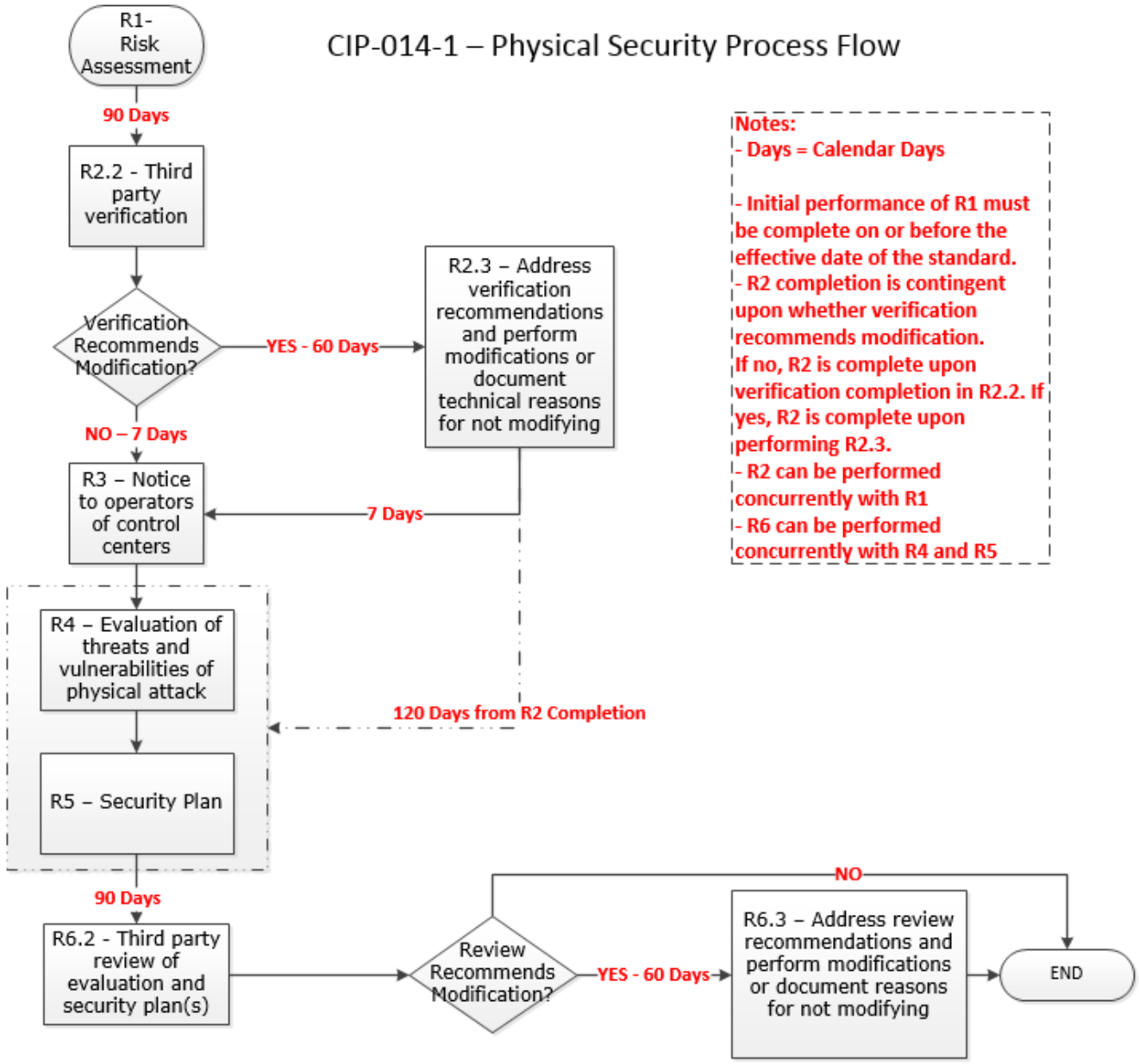
b. Why not "require" unaffiliated Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier of the Requirement R1 risk assessment?

The SDT considered whether to require Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier and decided against such a requirement. The SDT does not believe it is appropriate to require Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier. This conclusion is based the following: (i) unless necessary for reliability there should not be a requirement that requires one functional entity to require another functional entity to perform a task; (ii) there are sufficient entities qualified to verify the risk assessment without mandating additional tasks on Reliability Coordinators, Transmission Planners, and Planning Coordinators, and (iii) Requirement R2 provides Transmission Owners the flexibility to consider from many qualified entities.

c. Why is NERC or the Regional Entities not included as a verifier or reviewer?

Similar to reasons provided above for not mandating Reliability Coordinators, Transmission Planners, and Planning Coordinators to be the verifier, the SDT decided against a requirement that would specify NERC or Regional Entities to be the verifier or reviewer. The proposed Reliability Standard, however, does not preclude an entity from requesting NERC or its Regional Entity to be the verifying or reviewing entity under Requirements R2 and R6, respectively.

6. There are several deadlines in the proposed Reliability Standard to complete the risk assessment, third party verification, security plan(s), and third party review of the evaluation of threats and the security plan – can you illustrate this timeline?



7. Why does the proposed Reliability Standard state that the Transmission Owner can work concurrently with the verifier of the risk assessment or reviewer (and the Transmission Operator of the review) of the evaluation of threats and the security plan(s)?

The SDT recognized the value, effectiveness, and efficiency that may result in the Transmission Owner working side-by-side with its verifier, and the Transmission Owner and Transmission Operator, respectively, working side-by-side with its reviewer. Thus, for example, the Transmission Owner may first perform its Requirement R1 risk assessment for identification of Transmission stations and Transmission substations on its own, and then, in a second step, have the verifier conduct its verification of the risk assessment. If more efficient, the Transmission Owner may combine those steps by working side-by-side with the verifying entity to complete the risk assessment and the verification at the same time. It is expected that the selection of this concurrent approach will lessen misunderstandings, and likely be more effective and efficient. This side-by-side approach is equally applicable for conducting the risk assessment and verification under Requirements R1 and R2 and the evaluation of threats, development and implementation of physical security plan(s), and review under Requirements R4 through R6.

8. Given that the TO and TOP will be subject to unaffiliated third party review, does that change how compliance and enforcement will be conducted for this proposed Reliability Standard?

The SDT expects auditors will use their professional judgment to assess the third party reviews and rely on them to avoid duplication of efforts as is permitted by auditing standards. However, some degree of auditor due diligence related to the third party review is necessary to provide a sufficient basis for reliance on the work of others. Documentation regarding the qualification of third parties and the scope and nature of their reviews will help facilitate reliance for compliance auditors. The Notes to Auditor sections of the draft RSAW associated with proposed CIP-014-1 supports the concept of considering the effect of third party verifications and reviews on audit risk and related rigor of compliance procedures.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2014-04 Physical Security

Please **DO NOT** use this form for submitting comments. Please use the electronic form to submit comments on the draft CIP-014-1 Reliability Standard. The electronic comment form must be completed by 8:00 p.m. Eastern on **Thursday, April 24, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at or (609) 651-9455.

The project page may be accessed by clicking here.

Background Information

On March 7, 2014, the Federal Energy Regulatory Commission (FERC) issued an order directing NERC to submit for approval, within 90 days of the order, one or more Reliability Standards to address physical security risks and vulnerabilities of critical facilities on the Bulk Power System (BPS).[1]

In the order, FERC stated that the proposed Reliability Standard(s) should require entities to take a least the following three steps:

- Perform a risk assessment to identify facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading failures on the BPS.
- Evaluate the potential threats and vulnerabilities to those identified facilities.
- Develop and implement a security plan designed to protect against physical attacks to those identified facilities based on the assessment of the potential threats and vulnerabilities to their physical security.

Additionally, FERC directed that the proposed Standard(s) should also: (1) include a procedure that will ensure confidential treatment of sensitive or confidential information; (2) include a procedure for a third party to verify the list of identified facilities and allow the verifying entity, as well as FERC, to add or remove facilities from the list of critical facilities; (3) include a procedure for a third party to review the evaluation of threats and vulnerabilities and the security plan; and (4) require that the identification of the facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. The proposed Physical Security Reliability Standard(s) must be filed with FERC by June 5, 2014.

In response to the order, NERC staff and the Standards Committee (SC) worked together in order to develop an action plan for meeting the June 5, 2014 filing deadline. The SC approved several waivers to facilitate meeting the required timelines and seated the Standard Drafting Team (SDT) on March 21, 2014.

[1] *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

This posting solicits comment on proposed Reliability Standard CIP-014-1 Physical Security. The proposed standard responds to the directives from the FERC order, and a summary of those directives with explanation of how the approach addresses them is available in the "Consideration of Issues and Directives" document on the project page.

You do not have to answer all questions below. Enter comments in simple text format. Bullets, numbers, and special formatting will not be retained. Due to the expected volume of comments, the SDT asks that commenters consider consolidating responses and endorsing comments provided by another.

Questions

1. **Applicability**: The applicability of proposed CIP-014-1 starts with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a "medium impact" rating. The drafting team did not modify these criteria in their use under CIP-014-1, as they have been previously approved by stakeholders, NERC, and FERC. The SDT sought to ensure that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1. The team determined that slightly modified criteria could possibly result in confusion in application. The drafting team considered several other alternatives to refine the scoping in the applicability section, such as a particular kV threshold in addition to the other criteria; however, after significant discussion, the team found no technical or reliability basis for providing such limitiation. Importantly, by virtue of application of Requirement R1, the scope of the standard only applies to Transmission Owners that have Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers. Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In those cases, the entity only performs Requirements R1 through R2. When that results in a null set, Requirement R1 additionally provides that subsequent risk assessments may occur less frequently. Similarly, while Transmission Operators are also listed in the applicability section, by virtue of application of the requirements, only certain Transmission Operators that are notified under the standard's Requirement R3 have obligations under the standard. Do you agree with the applicability section? If not, please provide specific recommendations, ensuring to articulate how your suggested approach would not limit the applicability in such a manner as to inadvertently miss a facility that should be covered under the standard as specified in the FERC order on physical security.

☐ Yes
☐ No

Comments:

2. **Requirements R1 through R3**: The first three requirements of CIP-014-1 require Transmission Owners to: (1) perform risk assessments to identify through transmission planning analysis those Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers, that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; (2) arrange for a third party verification (as directed in the order) of the identifications; and (3) notify certain Transmission Operators of identified primary control centers that operationally control the identified and verified Transmission stations and Transmission substations. The requirements provide the periodicity for satisfying these obligations. Only an entity that owns or operates one or more of the identified facilities has further obligations in Requirements R4 through R6. If an entity identifies a null set after applying Requirements R1 through R2, the rest of the standard does not apply. Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.

☐ Yes
☐ No

Comments:

3. **Requirements R4 through R6**: The final three requirements of CIP-014-1 require (1) the evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified and verified according to the earlier requirements, (2) the development and implementation of a security plan(s) designed in response to the evaluation, and (3) a third party review of the evaluation and security plan(s) (as directed in the order). Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.

☐ Yes
☐ No

Comments:

4. Do you have input on other areas of the standard or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions. Please limit your response to 300 words or less.

☐ Yes
☐ No

Comments:

Consideration of Issues and Directives

Project 2014-04 - Physical Security

April 9, 2014

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that each Transmission Owner perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line was appropriate because it has been vetted with stakeholders, and approved by NERC and FERC. The SDT concluded it was a technically sound basis to determine which Transmission Owners should conduct the risk assessment. If the Transmission Owner does not have any Transmission stations or substations that meet the Medium Impact rating, it is not subject

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the methodology is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed,	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
operated, and maintained, and the sophistication of recovery plans and inventory management.		
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that each Transmission Owner and Transmission Operator that owns or operates facilities identified in accordance with Requirement R1 (and verified under Requirement R2) conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or threat warnings from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that each Transmission Owner and Transmission Operator that owns or operates facilities identified in accordance with Requirement R1 (and verified under Requirement R2) develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1) resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4; (2) law enforcement contact and

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		coordination information; (3) a timeline for implementing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the third party verifier under Requirement R2 or the reviewing entity under Requirement R6. These steps will help ensure that lists of critical facilities or other sensitive documents remain confidential.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a	*Reliability Standards for Physical Security*	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated entity verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a registered

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the verifying entity shall either verify the Transmission Owner's risk assessment or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The reviewing entity must be either (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file the plan with the Reliability Standards for Commission review.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

CIP-014-1 – Physical Security

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

Applicability of Requirements ***[RSAW developer to insert correct applicability]***

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1												X[3,4]			
R2												X[3,4]			
R3												X[3,4]			
R4												X[3,4]	X[4]		
R5												X[3,4]	X[4]		
R6												X[3,4]	X[4]		

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC orders, and the language included in this document, FERC orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

[3] Applicability is further defined to owners of transmission Facilities operated at 500 kV or higher (see section 4.1.1.1 of the Standard) and owners of certain transmission Facilities operating between 200 kV and 499 kV where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations, per section 4.1.1.2 of the Standard. In addition, sections 4.1.1.3 and 4.1.1.4 bring additional transmission Facilities identified as either critical to the derivation of Interconnection Reliability Operating Limits and Nuclear Plant Interface, respectively, within the purview of the standard. Please see the referenced sections of the Standard for additional details regarding applicability of the Requirements to Transmission Owners.

[4] Facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission are not subject to this Standard.

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Note to Auditors Concerning Third Party Verifications and Reviews

Requirements R2 and R6 prescribe, respectively, unaffiliated third party verifications for Requirement R1 and unaffiliated third party reviews for Requirements R4 and R5. Auditors are encouraged to rely on the verifications and reviews performed in cases where the verifying or reviewing entities are qualified, unaffiliated with the audited entity, and the scope of their verification or review is clear. The concept of reliance means using the work of others to avoid duplication of efforts and is consistent with recognized professional auditing standards, which are required for Compliance Audits per NERC's Rules of Procedure. Reliance in the context of this Reliability Standard means using the Requirement R2 verifications and Requirement R6 reviews to reduce audit risk and the related rigor of audit testing for Requirements R1, R4, and R5. However, in cases where the verifying or reviewing entity lacks the qualifications specified in Requirement R2 for verifications or Requirement R6 for reviewers, the required unaffiliation from the audited entity, or where the scope of the third party entity's verification or review is unclear, auditors may need to apply audit testing of Requirements R1, R4, or R5. For this reason, the Evidence Requested and Compliance Assessment Approach Sections are still present in this RSAW for Requirements R1, R4, and R5. We anticipate those sections will also facilitate expectations for entities and their unaffiliated third party verifiers and reviewers, assist Electric Reliability Organization (ERO) auditors to understand the audit procedures applied by unaffiliated third party verifiers and reviewers, and provide transparency between ERO auditors and Industry, should circumstances require audit testing of Requirements R1, R4, or R5. Further, it is an objective of the ERO to have transparent Evidence Requests and Compliance Assessment Approaches for every enforceable standard, whether they are in audit scope or not.

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1.The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2)one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1.

Registered Entity Response (Required):

Question: As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1? ☐ Yes ☐ No

☐ This entity does not have any applicable Transmission stations/substations.

☐ Other: [Provide explanation below]

[Include additional information regarding the question here, including the type of response and format of the response requested, as appropriate.]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R1) Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant).
(R1) List of existing Transmission stations/substations that meet the criteria specified in Section 4.1.1.
(R1) List of Transmission stations/substations planned in the next 24 months that meet criteria specified in Section 4.1.1.
(R1 Part 1.2) List of primary control centers that operationally control each identified Transmission station/substation.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R1

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review entity's process for determining Transmission stations/substations subject to identification in accordance with Requirement R1, including weighting described in Section 4.1.1.2.
	(R1) Review entity's risk assessment process to determine the Transmission stations/substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection.
	(R1) Ensure entity's risk assessment process includes Transmission stations/substations planned in the next 24 months.
	(R1) Ensure a risk assessment was performed for each Transmission station/substation meeting applicability described in Section 4.1.

	(R1 Part 1.1) If applicable, review any prior risk assessments and verify whether or not Transmission stations/substations were identified.
	(R1 Part 1.1) Review evidence that risk assessment was performed and verify that it occurred within the past 30 months where items were identified in the previous risk assessment and 60 months where no items were identified in the previous risk assessment.

Note to Auditor: Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary.

See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator;
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated verifying entity shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a s Transmission station or Transmission substation::

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated verifying entity.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R2) Dated evidence of third party verification of the entity's risk assessment performed under Requirement

R1.
(R2 Part 2.1) Documented qualifications of the verifying party.
(R2 Part 2.3) Recommendations, if any, of the verifying party related to Requirement R1 risk assessments.
(R2 Part 2.3) Documentation of modifications and implementation of recommendations or technical basis for not implementing recommendations of the verifying party.
(R2 Part 2.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R2) Review evidence of third party verification of the entity's risk assessment and verify the following:
	(R2 Part 2.1) The reviewing entity is registered in accordance with Part 2.1 or has transmission planning or analysis experience.
	(R2 Part 2.2) Verification was completed with 90 calendar days of risk assessment.
	(R2 Part 2.3) Verifying entity's recommendations, if any, were used to modify the entity's Requirement R1 identification or the technical basis for not modifying the Requirement R1 identification is documented within 60 calendar days of completion of the verification.
	(R2 Part 2.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between the entity and third party were implemented.
Note to Auditor See Guidelines and Technical Basis section of the standard and Rationale for Requirement R2 associated with the Standard for additional details regarding the term 'unaffiliated.' The third party verification may occur concurrent with or after the risk assessment performed under Requirement R1.	

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. For the primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Registered Entity Response (Required):

Question: Are any primary control centers identified in Requirement R1, Part 1.2 not under operational control of your NERC registration? ☐ Yes ☐ No

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R3) If applicable, dated communications with Transmission Operators demonstrating notification and the date of completion of Requirement R2.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R3

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R3) For each applicable primary control center identified in Requirement R1 Part 1.2 not under the control of the entity's registration, verify notification exists and contains the date of completion of Requirement R2.
	(R3 Part 3.1) For each Transmission station/substation removed under Part 3.1, ensure the responsible Transmission Operator was notified of the removal within seven calendar days of removal from identification.
Note to Auditor: Note the entity's response to the above Question. If auditor can verify the entity's answer of 'No,' then Requirement R3 is not applicable and no further audit testing is required.	

Auditor Notes:

.

R4 Supporting Evidence and Documentation

R4. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R4) A description of the entity's process for executing the evaluation prescribed in Requirement R4.
(R4) Dated evidence of the evaluation prescribed in Requirement R4.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R4

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence of evaluation and verify it considers the following:
	(R4) Potential threats as described in Requirement R4.
	(R4 Part 4.1) Unique characteristics as described in Requirement R4 Part 4.1.
	(R4 Part 4.2) Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
	(R4 Part 4.3) Intelligence or warnings as described in Part 4.3.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 to ensure it is complete.	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes:

5.1. Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating implementation of the physical security plan.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R5) Dated physical security plan(s).

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R5

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Review evidence and verify the physical security plan(s) covers the Transmission stations/substations and primary controls identified in Requirements R1 and/or R2, and verify plan was implemented within 120 calendar days following the completion of Requirement R2. In addition, verify the plan includes the following attributes:
	(R5 Part 5.1) Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of Requirement R4.
	(R5 Part 5.2) Law enforcement contact and coordination information.
	(R5 Part 5.3) A timeline for implementing physical security enhancements and modifications specified in the physical security plan.
	(R5 Part 5.4) Provisions to evaluate evolving physical threats, and their corresponding security measures in accordance with R5 Part 5.4
	(R5) Verify implementation of physical security plan(s). See 'Note to Auditor' for details.

Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities that would facilitate physical attacks that have a high probability or likelihood of occurrence.

Requirement R5 includes implementation of the security plan(s), which is not within the scope of the third party review described in Requirement R6. Auditors can gain reasonable assurance security plan(s) was/were implemented by determining if specific actions prescribed by the plan(s) have taken place within the timelines established by the plan(s). For example, if the plan calls for certain procedures to occur, then auditors could ask for evidence demonstrating the procedure has been implemented within the timeline established in the security plan. Also, if the plan calls for construction of a barrier, an auditor could verify evidence that such a barrier was constructed in accordance with the entity's timeline. As auditors should obtain reasonable, not absolute, assurance the plan(s) was/were implemented, testing implementation on a sample basis may be appropriate.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

6.1..1. An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.

6.1..2. An entity or organization approved by the ERO.

6.1..3. A governmental agency with physical security expertise.

6.1..4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated reviewing entity recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its security plan(s) consistent with the recommendation; or
- Document the reason for not modifying the security plan(s) consistent with the recommendation

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information exchanged with the unaffiliated reviewing entity.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3..

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R6) Dated Evidence of unaffiliated third party review of entity's Requirement R4 evaluation and Requirement R5 security plan(s).
(R6 Part 6.1) Evidence that reviewing entity staff meets qualifications identified in Part 6.1.
(R6 Part 6.3) Recommendations of reviewing party related to Requirement R4 evaluation and Requirement R5 security plan.
(R6 Part 6.3) Dated documentation of modifications and implementation of recommendations or reasons and compensating mitigating measures for not implementing recommendations of the reviewing party.
(R6 Part 6.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R6

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R6) Review evidence and verify the physical security plan(s) and the Requirement R4 evaluation have been reviewed by an unaffiliated third party. Also, review evidence and verify the following:
	(R6 Part 6.1) Reviewing party has the qualifications identified in Part 6.1.
	(R6 Part 6.2) Review is dated within 90 calendar days of completion of the Requirement R5 security plan.
	(R6 Part 6.3) Reviewing entity recommended changes to security plan(s) were made by entity or the reason(s) for not making the change(s) was/were documented within 60 calendar days of the completion of the unaffiliated third party review.
	(R6 Part 6.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between entity and third party were implemented.
Note to Auditor: The third party review may occur concurrent with or after the evaluation performed under Requirement R4 or the security plan develop under Requirement R5. See Guidelines and Technical Basis associated with the Standard for additional details related to qualifications of reviewing entities that may inform audited entities selection of a reviewing entity.	

Auditor Notes:

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of CIP-014-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's…….

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's…….

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	04/09/2014	Physical Security RSAW Task Force	New Document

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Formal Comment Period Now Open through April 24, 2014
Ballot Pools Forming Now through April 19, 2014

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

In an order issued March 7, 2014, the Federal Energy Regulatory Commission directed NERC to file a physical security standard within 90 days of the order (*i.e.*, by June 5, 2014). On March 21, 2014, the NERC Standards Committee (SC) authorized a waiver of the standard development process, in accordance with Section 16 of the Standard Processes Manual, to meet this pending regulatory deadline. The SC approved to shorten this comment period from 45 days to 15 calendar days, with a concurrent ballot conducted during the last 5 days of the comment period. The waiver also provided for ballot pool formation to begin immediately upon approval of the waiver, with closure of the ballot pool 10 days after the initial formal comment and ballot period begins. (Sections 4.7-4.9)

Now Available

A 15-day formal comment period for **CIP-014-1 – Physical Security** is open through **8 p.m. Eastern on Thursday, April 24, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455.

Background information for this project can be found on the project page. Please refer to the 1-page Project Overview to learn more about the Physical Security standard and project at a glance.

Instructions for Commenting

Please use the electronic form to submit comments on the standard. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for Project 2014-04 – Physical Security and the associated non-binding poll on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Initial Ballot: bp-2014-04_CIP-014-1_in@nerc.com
Non-Binding poll: bp-2014-04_CIP-014-1_NB_in@nerc.com

Next Steps

An initial ballot for the standard and non-binding poll of the associated VRFs and VSLs will be conducted **April 20-24, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Formal Comment Period Now Open through April 24, 2014
Ballot Pools Forming Now through April 19, 2014

This email distribution list may include individuals subject to ex parte communication restrictions pursuant to Rule 2201 of the Federal Energy Regulatory Commission's regulations governing off-the-record communications (18 C.F.R. § 385.2201 (2014)). Please refrain from using this distribution list for any substantive communications related to Project 2014-04, Physical Security.

In an order issued March 7, 2014, the Federal Energy Regulatory Commission directed NERC to file a physical security standard within 90 days of the order (*i.e.*, by June 5, 2014). On March 21, 2014, the NERC Standards Committee (SC) authorized a waiver of the standard development process, in accordance with Section 16 of the Standard Processes Manual, to meet this pending regulatory deadline. The SC approved to shorten this comment period from 45 days to 15 calendar days, with a concurrent ballot conducted during the last 5 days of the comment period. The waiver also provided for ballot pool formation to begin immediately upon approval of the waiver, with closure of the ballot pool 10 days after the initial formal comment and ballot period begins. (Sections 4.7-4.9)

Now Available

A 15-day formal comment period for **CIP-014-1 – Physical Security** is open through **8 p.m. Eastern on Thursday, April 24, 2014.**

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455.

Background information for this project can be found on the project page. Please refer to the 1-page Project Overview to learn more about the Physical Security standard and project at a glance.

Instructions for Commenting

Please use the electronic form to submit comments on the standard. If you experience any difficulties in using the electronic form, please contact Wendy Muller. An off-line, unofficial copy of the comment form is posted on the project page.

Instructions for Joining Ballot Pool

Ballots pools are being formed for Project 2014-04 – Physical Security and the associated non-binding poll on this project. Registered Ballot Body members must join the ballot pools to be eligible to vote in the balloting and submittal of an opinion for the non-binding poll of the associated Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs). Registered Ballot Body members may join the ballot pools at the following page: Join Ballot Pool

During the pre-ballot window, members of the ballot pool may communicate with one another by using their "ballot pool list server." (Once the balloting begins, ballot pool members are prohibited from using the ballot pool list servers.) The list servers for this project are:

Initial Ballot: bp-2014-04_CIP-014-1_in@nerc.com
Non-Binding poll: bp-2014-04_CIP-014-1_NB_in@nerc.com

Next Steps

An initial ballot for the standard and non-binding poll of the associated VRFs and VSLs will be conducted **April 20-24, 2014.**

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Initial Ballot and Non-Binding Poll Results

Now Available

An initial ballot for **CIP-014-1 – Physical Security** and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels concluded at **8 p.m. Eastern on Thursday, April 24, 2014.**

The standard achieved a quorum and sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballot.

Approval	Non-Binding Poll Results
Quorum: 88.60%	Quorum: 84.62%
Approval: 82.07%	Supportive Opinions: 83.83%

Background information for this project can be found on the project page.

Next Steps

The drafting team will consider all comments received during the formal comment period and, if needed, make revisions to the standard. If the standard does not show the need for significant revisions, it will proceed to a final ballot

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller (via email), Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	2014-04_CIP-014-1
Ballot Period:	4/20/2014 - 4/24/2014
Ballot Type:	Initial
Total # Votes:	404
Total Ballot Pool:	456
Quorum:	**88.60 % The Quorum has been reached**
Weighted Segment Vote:	82.07 %
Ballot Results:	**The ballot has closed**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	121	1	85	0.787	23	0.213	0	2	11
2 - Segment 2	8	0.6	6	0.6	0	0	0	1	1
3 - Segment 3	105	1	79	0.919	7	0.081	0	7	12
4 - Segment 4	38	1	27	0.871	4	0.129	0	2	5
5 - Segment 5	101	1	70	0.843	13	0.157	0	5	13
6 - Segment 6	60	1	49	0.907	5	0.093	0	0	6
7 - Segment 7	5	0.2	2	0.2	0	0	0	0	3
8 - Segment 8	6	0.6	2	0.2	4	0.4	0	0	0
9 - Segment 9	3	0.1	1	0.1	0	0	0	2	0

10 - Segment 10	9	0.6	4	0.4	2	0.2	0	2	1
Totals	**456**	**7.1**	**325**	**5.827**	**58**	**1.273**	**0**	**21**	**52**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke		
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Negative	COMMENT RECEIVED
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Hudson Gas & Electric Corp.	Frank Pace	Negative	COMMENT RECEIVED
1	Central Iowa Power Cooperative	Kevin J Lyons	Negative	COMMENT RECEIVED
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	COMMENT RECEIVED
1	Cleco Power LLC	Danny McDaniel	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Edison Electric Institute	David Batz	Affirmative	
1	El Paso Electric Company	Pablo Onate	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	COMMENT RECEIVED
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Negative	COMMENT RECEIVED
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	

1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	COMMENT RECEIVED
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	COMMENT RECEIVED
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John Chin	Abstain	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	John Burnett	Affirmative	
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Negative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton	Negative	SUPPORTS THIRD PARTY COMMENTS - (Please see comments submitted by me on behalf of the New Brunswick Power Corporation)
1	Network & Security Technologies	Nicholas Lauriat		
1	New York Power Authority	Bruce Metruck	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Negative	COMMENT RECEIVED
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	COMMENT RECEIVED
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Chelan County	Chad Bowman	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	

1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Affirmative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southwestern Power Administration	Angela L Summer	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES/SPP)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Negative	COMMENT RECEIVED
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Hudson Gas & Electric Corp.	James J McCloskey		
3	City of Anaheim Public Utilities Department	Dennis M Schmidt	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Mark Schultz	Abstain	

3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Abstain	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	East Kentucky Power Coop.	Patrick Woods	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
3	El Paso Electric Company	Rhonda Bryant	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	Entergy	Kevin Weber	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony		
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lee County Electric Cooperative	David A Hadzima		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	COMMENT RECEIVED
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Abstain	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	North Carolina Municipal Power Agency #1	Kathy Moyer	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi - OPPD)
3	Orange and Rockland Utilities, Inc.	David Burke		

3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Negative	COMMENT RECEIVED
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Chelan County	Steve Wickel	Affirmative	
3	Public Utility District No. 1 of Clallam County	Doug Adams	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Southern Indiana Gas and Electric Co.	Fred Frederick	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	SUPPORTS THIRD PARTY COMMENTS - (Please see TVA's comments submitted through the electronic comment form)
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott		
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	COMMENT RECEIVED
4	DTE Electric	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas	Affirmative	
4	Garkane Energy	Mike Avant		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Negative	COMMENT RECEIVED
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke		
4	National Rural Electric Cooperative	Barry R. Lawson	Abstain	

	Association			
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Affirmative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
4	Southern Minnesota Municipal Power Agency	Richard L Koch		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Acciona Energy North America	George E Brown	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Negative	SUPPORTS THIRD PARTY COMMENTS - (Black Hills Corporation on behalf of 4 entities)
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery	Abstain	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	COMMENT RECEIVED
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	East Kentucky Power Coop.	Stephen Ricker	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	El Paso Electric Company	Gustavo Estrada	Affirmative	

5	Electric Power Supply Association	John R Cashin		
5	Empire District Electric Co.	mike I kidwell	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Hydro-Québec Production	Roger Dufresne	Negative	SUPPORTS THIRD PARTY COMMENTS - (in support of HQT)
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lafayette Utilities System	Jamie B Webb		
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Manitoba Hydro	Chris Mazur	Negative	COMMENT RECEIVED
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	COMMENT RECEIVED
5	Ontario Power Generation Inc.	David Ramkalawan	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Chelan County	John Yale	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Illinois Power Coop.	Alvis D Lanton		
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	

5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	El Paso Electric Company	Luis Rodriguez	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw		
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Negative	COMMENT RECEIVED
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi)
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp	Affirmative	
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	

6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	COMMENT RECEIVED
6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Eastman Chemical Company	David L Moore		
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Praxair Inc.	David Meade		
7	Siemens Energy, Inc.	Frank R. McElvain	Affirmative	
7	Valero Services, Inc.	Lee W Morris		
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner	Negative	COMMENT RECEIVED
8		David L Kiguel	Negative	COMMENT RECEIVED
8	Foundation for Resilient Societies	William R Harris	Negative	COMMENT RECEIVED
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	COMMENT RECEIVED
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Idaho State Public Utilities Commission	Johanna Bell	Affirmative	
9	National Association of Regulatory Utility Commissioners	Jerry M Maio	Abstain	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC CIPC comments)
10	Southwest Power Pool RE	Bob Reynolds	Negative	COMMENT RECEIVED
10	Texas Reliability Entity, Inc.	Derrick Davis	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Non-Binding Poll Results

Project 2014-04 Physical Security CIP-014-1

Non-Binding Poll Results	
Non-Binding Poll Name:	2014-04_CIP-014-1
Poll Period:	4/20/2014 - 4/24/2014
Total # Opinions:	363
Total Ballot Pool:	429
Ballot Results:	84.62% of those who registered to participate provided an opinion or abstention; 83.84% of those who provided an opinion indicated support for the VRFs and VSLs that were proposed.

Individual Ballot Pool Results

Segment	Organization	Member	Opinions	Comments
1	Ameren Services	Eric Scott	Abstain	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Abstain	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke		
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Abstain	
1	Baltimore Gas & Electric Company	Christopher J Scanlon		
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen		
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Abstain	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Hudson Gas & Electric Corp.	Frank Pace	Negative	COMMENT RECEIVED
1	Central Iowa Power Cooperative	Kevin J Lyons		
1	City of Garland	David Grubbs	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Negative	COMMENT RECEIVED

1	Cleco Power LLC	Danny McDaniel	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Abstain	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Edison Electric Institute	David Batz		
1	El Paso Electric Company	Pablo Onate	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	COMMENT RECEIVED
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Abstain	
1	Gainesville Regional Utilities	Richard Bachmeier		
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	COMMENT RECEIVED
1	Idaho Power Company	Molly Devine	Affirmative	
1	International Transmission Company Holdings Corp	Michael Moltane	Abstain	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	
1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Negative	SUPPORTS THIRD PARTY COMMENTS - (Brett Holland)
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John Chin	Abstain	
1	Lincoln Electric System	Doug Bantam	Affirmative	

1	Los Angeles Department of Water & Power	John Burnett	Abstain	
1	Lower Colorado River Authority	Martyn Turner		
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Negative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton	Negative	SUPPORTS THIRD PARTY COMMENTS - (See comments from New Brunswick Power Corporation)
1	Network & Security Technologies	Nicholas Lauriat		
1	New York Power Authority	Bruce Metruck	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Negative	COMMENT RECEIVED
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Affirmative	
1	Platte River Power Authority	John C. Collins	Abstain	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (EEI)
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Abstain	
1	Public Utility District No. 1 of Chelan County	Chad Bowman		
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	

1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Abstain	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa		
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
1	Southwestern Power Administration	Angela L Summer	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES/SPP)
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Abstain	
1	Trans Bay Cable LLC	Steven Powell		
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	
1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo		
1	U.S. Bureau of Reclamation	Richard T Jackson	Negative	COMMENT RECEIVED
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper		
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		

3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist		
3	Arkansas Electric Cooperative Corporation	Philip Huff	Abstain	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	City of Anaheim Public Utilities Department	Dennis M Schmidt	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Abstain	
3	City of Green Cove Springs	Mark Schultz	Abstain	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee		
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla	Affirmative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Abstain	
3	DTE Electric	Kent Kujala	Affirmative	
3	East Kentucky Power Coop.	Patrick Woods	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
3	El Paso Electric Company	Rhonda Bryant	Affirmative	
3	Empire District Electric Co.	Kalem Long		
3	Entergy	Kevin Weber		
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Affirmative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	

3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		
3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Joshua D Bach		
3	Kissimmee Utility Authority	Gregory D Woessner	Abstain	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lee County Electric Cooperative	David A Hadzima		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert		
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Negative	COMMENT RECEIVED
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Abstain	
3	Muscatine Power & Water	John S Bos		
3	National Grid USA	Brian E Shanahan	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Abstain	
3	Nebraska Public Power District	Tony Eddleman	Abstain	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	North Carolina Municipal Power Agency #1	Kathy Moyer	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi - OPPD)
3	Orange and Rockland Utilities, Inc.	David Burke		
3	Orlando Utilities Commission	Ballard K Mutters	Abstain	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Abstain	
3	PNM Resources	Michael Mertz	Negative	COMMENT RECEIVED
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Abstain	

3	Public Utility District No. 1 of Chelan County	Steve Wickel	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Abstain	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Southern Indiana Gas and Electric Co.	Fred Frederick	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey		
3	Tennessee Valley Authority	Ian S Grant	Abstain	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott		
3	Westar Energy	Bo Jones	Affirmative	
3	Xcel Energy, Inc.	Michael Ibold	Abstain	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell		
4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	COMMENT RECEIVED
4	DTE Electric	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Abstain	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Garkane Energy	Mike Avant		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen		
4	Illinois Municipal Electric Agency	Bob C. Thomas	Abstain	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Abstain	
4	Modesto Irrigation District	Spencer Tacke		
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen		

4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Abstain	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Abstain	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Acciona Energy North America	George E Brown	Abstain	
5	Amerenue	Sam Dwyer	Abstain	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Negative	SUPPORTS THIRD PARTY COMMENTS - (Black Hills Corporation on behalf of 4 entities)
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Affirmative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Calpine Corporation	Hamid Zakery	Abstain	
5	City and County of San Francisco	Daniel Mason	Abstain	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose		
5	Cleco Power	Stephanie Huffman	Negative	SUPPORTS THIRD PARTY COMMENTS - (See SPP Group)
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	COMMENT RECEIVED
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		

5	Dominion Resources, Inc.	Mike Garton	Abstain	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	
5	East Kentucky Power Coop.	Stephen Ricker	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	El Paso Electric Company	Gustavo Estrada	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Empire District Electric Co.	mike l kidwell		
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper		
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS - (ACES)
5	Hydro-Québec Production	Roger Dufresne	Negative	SUPPORTS THIRD PARTY COMMENTS - (in support of HQT)
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Negative	COMMENT RECEIVED
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lafayette Utilities System	Jamie B Webb		
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Manitoba Hydro	Chris Mazur	Negative	COMMENT RECEIVED
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Abstain	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Abstain	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	

5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Negative	COMMENT RECEIVED
5	Ontario Power Generation Inc.	David Ramkalawan	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Abstain	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Abstain	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Illinois Power Coop.	Alvis D Lanton		
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Abstain	
5	Tennessee Valley Authority	David Thompson	Negative	COMMENT RECEIVED
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Negative	COMMENT RECEIVED
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Abstain	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Negative	SUPPORTS THIRD PARTY

				COMMENTS - (See SPP Group)
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson		
6	Duke Energy	Greg Cecil	Affirmative	
6	El Paso Electric Company	Luis Rodriguez	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson		
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Negative	COMMENT RECEIVED
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw		
6	Luminant Energy	Brenda Hampton	Abstain	
6	Manitoba Hydro	Blair Mukanik	Negative	COMMENT RECEIVED
6	Modesto Irrigation District	James McFall	Abstain	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Negative	SUPPORTS THIRD PARTY COMMENTS - (Mahmood Safi)
6	PacifiCorp	Sandra L Shaffer	Abstain	
6	Platte River Power Authority	Carol Ballantine	Abstain	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp	Affirmative	
6	Powerex Corp.	Gordon Dobson-Mack		
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Abstain	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Abstain	
6	Sacramento Municipal Utility District	Diane Enderby	Abstain	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Affirmative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	

6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard		
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Abstain	
6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
7	Eastman Chemical Company	David L Moore		
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Praxair Inc.	David Meade		
7	Siemens Energy, Inc.	Frank R. McElvain	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner	Abstain	
8		David L Kiguel	Negative	COMMENT RECEIVED
8	Foundation for Resilient Societies	William R Harris		
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	COMMENT RECEIVED
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Idaho State Public Utilities Commission	Johanna Bell	Affirmative	
9	National Association of Regulatory Utility Commissioners	Jerry M Maio	Abstain	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Negative	SUPPORTS THIRD PARTY COMMENTS - (SERC CIPC comments)
10	Southwest Power Pool RE	Bob Reynolds	Negative	COMMENT RECEIVED
10	Texas Reliability Entity, Inc.	Derrick Davis	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Abstain	

Individual or group. (137 Responses)
Name (97 Responses)
Organization (97 Responses)
Group Name (40 Responses)
Lead Contact (40 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (35 Responses)
Comments (137 Responses)
Question 1 (94 Responses)
Question 1 Comments (102 Responses)
Question 2 (96 Responses)
Question 2 Comments (102 Responses)
Question 3 (93 Responses)
Question 3 Comments (102 Responses)
Question 4 (95 Responses)
Question 4 Comments (102 Responses)

Individual
Jennifer Wright
San Diego Gas & Electric
Yes
San Diego Gas & Electric (SDG&E) agrees that it is appropriate to start with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a “medium impact” rating. However, SDG&E believes that it would be prudent to simply refer to the CIP-002-5.1 Impact Rating Criteria rather than restating it in CIP-014 Standard. Being more specific that this Standard is applicable to Transmission Owners that have any facilities identified as “medium impact” facilities under CIP-002-5.1 Attachment 1, Inpact Rating Criteria 2.4, 2.5, 2.6 and 2.7, would be clearer and more consistent with the general way that CIP-003-5 through CIP-011-5 are built upon the identification of “critical” facilities made in CIP-002-5.1. Linking the two explicitly, rather than simply restating the same language, would prevent the possibility that differences could creep into the rules over time as each Standard is modified.
Yes
SDG&E agrees with this approach. A facility’s identification as “medium impact” does not necessarily mean that the facility, if rendered inoperable or damaged could result in widespread instability, uncontrolled separation or Cascading within an Interconnection. Application of a risk assessment will ensure that CIP-014-1 is focused on the facilities that are most critical to the system.
Yes

SDG&E agrees that an evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified in R1 through R3 of the Standard is appropriate. Security threats and vulnerabilities can, and will vary from location to location and such differences must be accounted for in a robust security plan. It is appropriate and necessary that the Standard not mandate a one-size-fits-all approach, but requires entities to take into account the unique characteristics of each facility. SDG&E understands the Federal Energy Regulatory Commission's concern addressed by its Paragraph 11 directive that the Standard must have the analysis verified by an independent third party. While SDG&E believes it has in-house experts capable of performing such an analysis (as required by R4) and developing a Physical Security plan (as required by R5) adequately, SDG&E appreciates that verification by a third party, essentially a "second opinion," can serve to ensure a robust analysis of the physical security threats and vulnerabilities of facilities identified in Requirements R1 through R3. SDG&E appreciates the broad definition under R6.1 of what qualifies as a "unaffiliated third party reviewer." A list that unnecessarily limits possible reviewers could: 1) result in a bottleneck as too few potential reviewers are available for the industry to use; and 2) result in increased costs and a tight market for reviewers results in higher prices for their services.
No
Individual
Debra Horvath
Portland General Electric
Yes
Yes
The following comments relate to suggested modifications for Requirements 1-3 – PGE believes the 90-day period to ensure verification of the risk assessment is too short. It will be difficult for every Transmission Owner to establish a contract with an unaffiliated verifying entity during the implementation time period. In addition, the current wording of the standard puts the obligation on the Transmission Owner to make sure that the assessment is done within 90 days, even though by definition they cannot have control over that timeline. Therefore, PGE proposes replacing the R2.2 language, "[t]he Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment," with the language, "[t]he Transmission Owner shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from the completion of the Requirement R1 risk assessment." In addition, Requirement R3 provides no mechanism for the Transmission Operator who operates a primary control center identified by a different Transmission Owner to disagree with that identification. PGE proposes including similar language to that in R2.3 to allow for the Transmission Operator to document the technical basis for not identifying its primary control center as an asset to be protected.
Yes

In Requirement R4 the phrase “owns or operates” is used for the first time. If Transmission Owner Entity A is also a Transmission Operator of a line it does not own, and that line was identified by Transmission Owner Entity B in Requirement R1 and verified according to Requirement R2, Entity A could be responsible for evaluating and protecting that line under this wording. However, there is no mechanism built into the standard to communicate this information or to allow the Transmission Operator to dispute the decision. In addition, Requirement R4.2 should be changed to “[p]rior history of attack.” In addition, in Requirement R4.3, the current wording places an unrealistic and unclear burden on every Transmission Owner to monitor intelligence or threat warnings from an open-ended list of sources. We recommend changing the wording from “[i]intelligence or threat warnings from sources” to “[i]intelligence or threat warnings received from sources” to narrow the obligation to information that the Transmission Owner actually received from its monitoring activities. In addition, in Requirement R5, the phrase “owns or has operational control over” is used for the first time. It’s not clear why this needs to be different from the “owns or operates” in Requirement R4. Consistent terms should be used to decrease potential confusion. In addition, as above, PGE believes that the 90-day period to review each entity’s evaluation and security plan is too short. Again, we propose replacing the R6.2 language, “[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5,” with the language, “[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from completing the security plan(s) developed in Requirement R5.”
No
Group
Tennessee Valley Authority
Brian Millard
Yes
Yes
No
Comment: Proposed language to be added to the end on Requirement 6: This Requirement shall not apply to any Federal corporation or agency that meets any of the criteria in Requirement 6.1 and that has an Inspector General, pursuant to the Inspector General Act Amendments of 1988, appointed by the President of the United States and charged with oversight responsibility for such Federal corporation or agency. Comment: Recommend adding “with electric utility experience” as a reviewer qualification to 6.1.3 and 6.1.4.

Rationale: There should be a common standardizing qualification such as PSP, CPP, or electric utility experience that applies across the sub requirements of R6 that entities and the ERO can use as criteria to qualify unaffiliated third party reviewers.
No
Individual
Guy Zito
Northeast Power Coordinating Council
No
The applicability of the draft standard should be expanded to incude Planning Coordinators in addition to Transmission Owners and Transmission Operators. While NPCC agrees that TOs and TOPs simple application of the screening criteria to determine which facilities need analysis, they may not be able to conduct a complete analysis. The SDT should consider that Transmission Owners in some cases do not have the ability to conduct an analysis with a "wide area" view of consequences. Smaller TOs or TOPs only have an outside equivalent representation of the BES and could need help conducting their analyses. Consideration should be given to allow them to conduct the studies in conjunction with PCs.
No
The Rationale Box for Requirement R2 stipulates that "'unaffiliated' means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission o(O)wner)." This conflicts with Requirement R2 Part 2.1 which lists "A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or An entity that has transmission planning or analysis experience" as those qualifications for an unaffiliated verifying entity. Clarification is needed that an Independent System Operator that has operating authority over an entity is eligible to be the unaffiliated verifying entity.
No
Regarding Part 5.1, the requirement states that the security measures should be designed to deter, detect, delay, assess, communicate and respond to potential physical threats. NPCC suggests removing the obligation to 'deter' from this Part and establish a separate Part that addresses deterrence and very basic specifics regarding what constitutes deterrence. The new Part could describe how an entity should implement deterrence and consider some minimum auditable criteria; for example, Consider and Implement measures designed to deter potential physical threats including 1) perimeter control 2) motion detection 3) lighting 4) access control. In this manner the ambiguity surrounding the term 'deter' is eliminated. Part 5.3 should allow flexibility to modify the time line. Suggest that Entities should 1) have a master Physical Security Plan; 2) have the flexibility to accomplish mitigation activities associated with the results of the vulnerability assessment, and 3) capture those mitigation plans under a separate mitigation plan (similar to the action plans for Cyber Assets vulnerability assessments) or include "associated modifications to the time line".

Yes
It is NPCC's expectation that RAI concepts will be applied to the operating and enforcement of this standard.
Individual
Greg Froehling
Rayburn Country Electric Cooperative
No
Overall comment is this is too complicated of a draft standard for a 90 day consensus! Keep it simple. I agree with the functional entitiy that is identified however, I would add GO to address any "critical" switchyards that may exist that are not owned by a TO. I also agree with the scoping of the facilities similar to the CIP V5 criteria with the following exception, apparently a list already exists for the substations that should be considered "high" do they deserve an alternative approach to what is within this standard? Altering the existing basic approach as follows: Since the FERC order allowed for "One or More Reliability Standards", it would be appropriate to address the "High " facilities separate from the "Medium Facilities". This approach would make it an easier task to file the "high standard" within the 90 days then follow with the "medium later". Thus giving more time, latitude and maneuverability to address issues that arise specific to those facilities.
No
I agree with the risk assessment in concept, the standard has far too many requirements and sub requirements to accomplish the task. Since initial analysis apparently this has already been done for the "High Risk" stations, a more efficient approach would be for the RC to perform the analysis based on the criteria mentioned to validate findings and find any second contingency facilities that may not have been identified. Since the RC is the "Reliability Coordinator", this is your third party identifying facilities without bias… Determinations will be based on an engineering basis utilizing standard uniform criteria across North America. The same analysis occurs for all entities within all regions, no variations this would yield consistency! Then the RC notify the entities that they have facilities that have been identified. (much like other NERC standards) Thus the information on which facilities have been identified would disseminated and controlled in a much more secure and better controlled environment while still maintaining the quality and consistency of the study needed.
No
Once the in scope facilities have been identified, it would be best for the entites to use the same resources for the evaluation of "Potential Threats" since this language has endless possibilities. i.e. Aerial attack, induced seismic events to name a few to illustrate "Potential". I favor the wording of "reasonable risks" The FBI, DOE or DHS should be involved in the discussion with the entities in lieu of a third party who is only subject to confidentiality agreements and also has interests beyond mitigating the true risks.
Yes

I think the standard IF broken up into 2 standards (High, Med) should provide clearer guidance as to the expectations of the plans content. Similar to the issues that arose with the Low assets in CIP V5 . Give basic structure and content to be addressed to give FERC the assurance the specific concerns have been met.
Individual
William H. Chambliss, member Operating Committee
Virginia State Corporation Commission
Yes
Yes
There does not seem to be any timeframe within which the initial assessment is to be completed under R1, nor when the 30 and 60 month periods for subsequent reassessments under R1.1 are to begin and conclude.
No
R4.2 requires each Transmission Owner of an identified facility to "consider" and "Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events." Is such consideration to be given to other "similar facilities" of the specific Transmission Owner or of any Transmission Owner anywhere in North America? How will such "consideration" be possible if the scope of such consideration is intended to be the latter? R5 is fine, but R6 suffers from the same ambiguity as R4.
No
Group
None
Terry Volkmann
Yes
No
The SDT has not factored in the resiliency concerns stated in the FERC order. Many of the facilities selected by the initial screening process will have long lead time equipment that if damaged will be out of service for several months. The assessment process needs to consider the operational risks during the time that the TO is waiting for replacement equipment. R1 should be amended to include the following sub-requirement. If the facility being studied has long lead time items, i.e. 4 months or greater, the study must include an N-1 analysis for the widespread instability, uncontrolled separation, or Cascading within an Interconnection test. In addition, the premise for this standard is a physical attack resulting in faulted equipment. There is no mention of the assessment being conducted for the Facilities under fault

conditions and in many cases under delayed clearing. R1 should be amended to include the following sub-requirement. The analysis of the subject Facility must include dynamic simulation of faulted conditions with delay cleared for the most severe contingency within the Facility. The phrase "instability, uncontrolled separation, or Cascading" is core to the definition of Interconnected Reliability Operating Limit (IROL). Every RC and PC has an IROL methodology under the FAC standards. R1 should be amended to include the following sub-requirement. The test for instability, uncontrolled separation, or Cascading must be consistent with the IROL methodology established by PCs and RCs under FAC-010 and FAC-011.
No
It is recognized that a one–size–fits all approach is not practical. However the proposed directives as to what should be included in physical security plans are so general that little is likely to change from current practices that are insufficient to protect very critical high risk substations. The only language directive in CIP-01401 is listed on Pg. 10, R5 para 5.1. More definitive guidelines must be outlined if improvements are to really be achieved. The utility industry has used real-time remote monitoring of substation equipment for reliability purposes for decades. Similar technology is available for the very important physical security function. The following sentence needs to be added at the end of paragraph 5.1. “Security measures must include isolation zones of sufficient size covering approaches to substations, in addition to monitoring inside substation fenced areas, to detect both attempted and actual penetration of critical sites and the surrounding buffer areas. The areas must be patrolled with real time monitoring & assessment equipment designed to provide live and playback/recorded video that must be automatically presented to alarm station operators. Detection equipment must include gunshot detectors. Sufficient real-time surveillance must be provided to allow sufficient time to implement a tactical response plan to minimize and interrupt threats.”
No
Individual
Steve Hamburg
Encari
Historically, FERC and NERC have taken the position that redundancy is not an acceptable criterion to exempt a Critical Cyber Asset from mandated physical or cyber controls. Redundancy is not supposed to be a factor in the determination of the criticality; instead redundancy is used to improve reliability and availability. This principle should be extended to the protective measures applicable to control centers under CIP-014-1. So long as both the primary control center and backup control centers meet the bright line criteria for a medium impact rating under CIP-002-5.1, the protections under CIP-014-1 should apply equally to both the primary and backup control centers.
No

There should be a strong, rebuttable presumption that an applicable Transmission Facility requires physical protection owing to its classification under the bright-line "medium impact" rating criteria under CIP-002-5.1 (which is repeated in the Applicability section of CIP-014-1 for Transmission Facilities). The utility of a risk assessment could be recognized, however, as justification for rebutting the presumed need for a set of mandated physical security measures.
No
The approach taken by the Nuclear Regulatory Commission, which prescribes specific physical protections for nuclear plants and materials in 10 CFR Part 73, is instructive. Applicable Transmission Facilities, which are subject to common potential threats and vulnerabilities, warrant minimum physical security protective measures. Physical security plans should incorporate those prescribed protective measures unless a responsible entity can establish that its validated security plan provides a comparable level of protection required by the Standard.
Yes
CIP-014-1 should expressly permit one well-coordinated physical security plan for a Transmission Facility. As proposed, there could be a separate physical security plan under CIP-006-5 for BES Cyber Systems within an applicable Transmission Facility and potentially another physical security plan for the Transmission Facility as whole under CIP-014-1.
Individual
David Ramkalawan
OPG
No
In the applicability section of the proposed standard, does the exemption refer to the Nuclear Generation Facility or the Transmission facility to which the Nuclear Generation Facility is connected? In Canada the Canadian Nuclear Safety Commission has no jurisdiction over the Transmission Owner/Operator; therefore the intent of the standard has to be made clear on this point.
Yes
Yes
Yes
Individual
Ralph Meyer
The Empire District Electric Company
Yes

EDE feels this is the right approach on selecting a threashold for applicability to this standard.
Yes
Yes
No
Individual
Kalem Long
The Empire District Electric Company
Yes
Yes
Yes
Yes
Individual
Mike Kidwell
Empire District Electric Company
Yes
Yes
Yes
Yes
Individual
Candace Morakinyo
We Energies
Agree
Edison Electric Institute (EEI)
Individual
Ronnie C. Hoeinghaus

City of Garland
Yes
Yes
No
Clarification - R6.2: Need to clarify that “completing the security plan(s)” does not include completing the tasks outlined in the time line developed in R5.3 – the time line is required to be complete as part of the plan but not the tasks in the time line.
Yes
Recommendation # 1 – Include the timeline diagram located in the FAQ document titled “CIP-014 Physical Security Process Flow” in the Guideline and Technical Basis section of the standard. This diagram clearly demonstrates the timing between the different requirements. Because of the subsequent risk analysis’s in R1, verifications in R2, and potentially the processes outlined in R3, R4, R5, & R6, questions on timing (answered by the diagram) potentially will arise throughout the life of the standard. Recommendation # 2 – Add the words “catastrophic failure” to the Purpose statement. On a webinar, there was discussion concerning the Purpose statement and it was stated a number of times that “widespread instability, uncontrolled separation” meant to convey the concept of “catastrophic” – there will be a lot of folks involved in the implementation of the standard who did not hear the webinar comments. Recommendation # 3 – Rather than the term “primary control center” used in all the proposed requirements, use a different term or phrase such as the “facility that has direct Supervisory Control”. The word “direct” in the recommendation of “direct Supervisory Control” should replace the need for the word “primary” - primary makes one think of primary and backup (which is not addressed in the standard). The concern with using primary control center, even though “control center” is not capitalized, brings up a mental picture of primary (and backup) Control Centers as defined in the NERC glossary. The standard should be straight forward, not using terms that can be confused.
Individual
David Rudolph
Basin Electric Power Cooperative (BEPC)
Yes
Yes
R2 – A concern to consider is whether there is an adequate pool of unaffiliated third party verifiers to meet the 90 day timeframe. Possible solutions would include (1) increase the 90 day requirement to six months; or (2) Revise the requirement to allow the NERC Registered Entity to notify the appropriate Regional Entity of the verifier pool constraint and request the Regional Entity act as the verifier or specify an acceptable alternative.

Yes
Yes
The SDT should be applauded for the diligent work performed in short order to meet the requirements of the FERC order RD14-6-000 while allowing flexibility in the manner the Registered Entity may be compliant.
Group
Edison Electric Institute
David Dworzak
Yes
Yes
Yes
Yes
EEI supports the draft standard CIP-014-1 as fully responsive to the FERC March 7 order. The project has moved along a very aggressive timeline and naturally raises a broad range of practical and implementation issues. Based on extensive discussions with member companies, EEI recommends that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify for companies several questions on the timing of the various implementation stages of the standard, including especially that security plans are subject to change over time for a broad range of reasons. In addition, EEI asks the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. Observing the many meetings and webinars that have taken place recently, EEI also recommends that the SDT consider adding language in the implementation guidance around the application of the terms 'control center,' 'primary control center,' and 'transmission station' in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies' ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms.
Group
Southwest Power Pool Regional Entity
Bob Reynolsa
No

SPPRE does not agree with the applicability because it excludes certain facilities that could pose a significant risk to the BPS reliability if rendered inoperable or damaged as a result of a physical attack. Other facilities that should be applicable are those where high impact BES Cyber Systems are found. Additionally, any Special Protection System and automatic load shedding system capable of shedding 300 Mw or more should be included. Reference CIP-002-5 Attachment 1 (Impact Rating Criteria 1.1, 1.2, 1.4,2.9, and 2.10). SPPRE also disagrees with the decision to limit applicability to only the primary control center.
No
SPPRE believes that greater clarity is required with respect to the risk assessment to be performed. At a minimum an extreme contingency study needs to be performed that takes out the entire facility, all voltages present. The study should also not consider any operating guides or other mitigation when evaluating the impact of the outage. In Section 2.3 technical basis should be changed to engineering basis. Additionally, the unaffliated verifying entity should not be the party performing the original study, under the principle that an auditor cannot audit ones own work; to do so would not be consistent with the expectation of verification by an unaffiliated entity.
No
SPPRE disagrees with the inclusion of Requirement 4.2. Prior history is not a predictor of future events and could result in critical facilities not being protected until after a sucessful first damaging attack with adverse BES reliability impact. Requirement 5.3 should be a project plan with measurable milestones for implementing the physical security enhancements and modifications.
Yes
SPPRE recommends that subsequent risk assessments should be peformed at least every 36 calendar months regardless of whether previous risk assessments had identified critical facilities. It is more important to identify facilities that should be on the list than those that might not need to be on the list anymore.
Individual
Randi Nyholm
Minnesota Power
Yes
Yes
Yes
Overall Minnesota Power agrees with the approach laid out by the Standard Drafting Team in Requirements 4-6, but requests that the SDT consider modifying the wording of R5.1 as follows. Resiliency or security measures designed to deter, detect, delay, assess, communicate, or respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4. An auditor could interpret the use of “and” in

"…deter, detect, delay, assess, communicate, and respond…" to mean that each resiliency or security measure be designed to meet all of these, where we believe and hope that the intent of the sub-Requirement is that the resiliency or security measure identified in the physical security plan be designed to "…deter, detect, delay, assess, communicate, or respond…", while recognizing that it may meet more than one.
No
Individual
Bob Thomas and Kevin Wagner
Illinois Municipal Electric Agency
Agree
Florida Municipal Power Agency American Public Power Association
Individual
Jack Stamper
Clark Public Utilities
No
Section 4.1.2 of the Applicability section states "Transmission Operator." This reference in the Applicability section should be more specific based on the the actual conditions under which CIP-014 would be applicable to a Transmission Operator. Clark suggests the reference should be revised to "Transmission Operators that have operational control over the primary control center of a Transmission station or Transmission substation identified in section 4.1.1."
Yes
Yes
No
Individual
Frank Pace
Central Hudson Gas & Electric Corporation
Yes
No
In regards to R2.2 as currently drafted, the unaffiliated verifying entity should have to ensure verification within 90 days and not the TO, since it is that entity performing the verification. In regards to R2.3 as currently drafted, there appears to be a lack of an appeals process in cases

of disagreement between the unaffiliated verifying entity and the TO concerning the recommendations formulated by the unaffiliated verifying entity.
Yes
No
Individual
Earl F. Cass
EF Cass Consulting Inc.
No
the applicability section table should be modified by either removing the 500kV line or making it a 3000 value. By giving it a 0 value in the table it send a different message than the text indicating all 500kV facilities are in. Also, in the draft RSAW Compliance Assessment approach for R1, it would appear that a Transmission Owner needs to comply with R1 and R2 in order to determine if the standard applies to them. If an entity is required to have a process for determining applicability then it needs to be a requirement. The applicability section should produce a yes or no answer. I spoke with Nick Webber of WECC and his response back was "Much like the requirement of all entities to apply CIP-002, all entities registered as for the TO function must complete CIP-014-1 R1 and R2. Each TO must complete R1 to determine if R3-R6 apply. The TO then must subsequently have that R1 assessment reviewed as required in R2." An entity should not have to comply with 2 of the requirements in order to determine if the standard applies to them. If all TOs are expected to comply with R1 and R2, then move the criteria into the requirement, if that is not the intent, clarify that once an entity reviews the applicability section and determines the standard does not apply they are finished. The rationale for requirement R1 indicates the criteria is in R1 when it is actually in the Applicability section.
Yes
This standard has the perceived importance of protecting national security and being so critical as to expedite its development through modification of nearly all associated controls. I agree physical security of critical facilities is of paramount concern but not at the expense of producing a sound standard. After listening to two of the webinars it is clear to me that the majority of the entities responsible for ultimately complying with this standard and those that will enforce the requirements are unclear as to what is required. I would suggest running it past the "Experts" for their review prior to the first vote.
Group
Tampa Electric Company
Ronald L Donahey

Yes
Yes
Yes
Comments to R5 Tampa Electric Company appreciates the excellent work of the standard drafting team (SDT). They and their support staffs have evidently worked very hard to produce in a very short time a family of documents that create a workable framework for improving the physical security of Transmission substations and primary Control Centers. We also commend NERC and the SDT for reaching out to the industry through a live a technical conference and by conducting a series Webinars in local and national venues. Moreover, we fully support the intent of the SDT as it has been articulated so well in the technical conference, in NERC and FRCC Webinars and in EEI and NATF conference calls. Unfortunately, there is a critical ambiguity in the text of requirement R5 that is problematic and needs to be addressed by the SDT. Our main concern is that requirement R5 literally reads that all provisions of the security plans for our primary control center and for all our substations and switchyards, including the installation and construction of any physical security upgrades, must be completed "within 120 calendar days following the completion of Requirement R2." Such a requirement may well be impossible to meet depending on the extent of the upgrades, the need for facility outages, and the number of locations that are affected. Members of the SDT have made it very clear in the Webinars and conference calls that they did not intend this result. Instead, the SDT intended to require registered entities, "within 120 calendar days following the completion of Requirement R2," to develop and document plans that include definite timelines for completing any security upgrades that are necessary to protect against the vulnerabilities and threats that are identified under requirement R4. Given that the text of R5 is contrary to the intent of the SDT, Tampa Electric urges the SDT to clarify that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. This clarification can be accomplished in the guidance document to the standard or by our preference, editing the text of the standard and issue a revised standard for a second ballot. Removing "and implement" from the text of requirement R5 should remove the ambiguity and conform the text to the intent of the SDT. This edit, combined with R5.3 expresses the SDT's intent on this issue: R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following

attributes: [VRF: High; Time-Horizon: Long-term Planning] 5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.

Yes

Comments: Comments to Definitions Tampa Electric also urges the SDT to define certain terms that appear in the standard: 1) “Transmission substation” and “Transmission station,” 2) “collector bus,” and 3)“primary control center. There terms are not defined in the NERC Glossary and may not have definitions that are universally accepted by the industry. “Transmission substation” and “Transmission station” Many industry practitioners use the term “Transmission substation” generally, whether or not any transformers are installed in the facility they are describing. Other practitioners apply the term “Transmission substation” only to facilities that include transformers. The standard implicitly uses the term “Transmission station” in reference to transmission switching arrangements that do not involve transformers. However, the more commonly used term for a transmission switching arrangement that does not include transformers is “Transmission switchyard.” NERC addressed this issue in the Guidelines and Technical Basis section of CIP-002-5. The SDT could easily carry that text over to the Guidelines and Technical Basis section of CIP-014-1. However, it would be better to add definitions for “Transmission substation” and “Transmission station” to the Glossary of Terms Used in NERC Reliability Standards. The relevant text in CIP-002-5 is copied below for the convenience of the SDT. CIP-002-5 Guidelines and Technical Basis clarifications of “Transmission stations” and “Transmission substations” The SDT uses the phrases “Transmission Facilities at a single station or substation” and “Transmission stations or substations” to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both “station” and “substation” to refer to the locations where groups of Transmission Facilities exist. “Collector bus” “Collector bus” is another term that is not defined in the NERC Glossary and that may not have a definition that is universally accepted by the industry. “Collector bus” appears in 4.1.1.1 and in 4.1.1.2. of CIP-014-1 in text that was carried over from CIP-002-5. 4.1.1 Transmission Owner that owns any of the following: 4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added] 4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added] If “Collector bus” is not defined or clarified, some TOs may conclude that some part of

every transmission substation or switchyard that receives the output of a generator(s) is excluded from the scope of the standard. However, that is not the case nor the intent of the SDT. Therefore, the drafting team should consider whether it should define or clarify in the guidance document, the term “collector bus” “Primary control center” The NERC Glossary defines “Control Center” in this manner: One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations. What might not be clear for the purposes of CIP-014-1 is what exactly distinguishes a “primary control center” from other alternate “Control Centers.” Some registered entities can operate substations from multiple locations. Often, there is one self-designated “main control center” or “primary control center” for which there might be multiple alternate or “backup control centers.” Given that alternate or backup control centers have capabilities that are comparable to so-called main control centers, it might not be clear in some systems whether “primary control center” in CIP-014-1 applies to more than one Control Center. The SDT can solve this problem by adding a definition of “primary control center” to the NERC Glossary or by adding text to CIP-014 that for each critical substation the TO or TOP can designate any Control Center as the “primary control center.”

Group

Black Hills Corporation Entities

Bob Case - NERC Compliance Manager , Bob.Case@blackhillscorp.com

No

Black Hills Corporation (referred to as BHC hereafter) believes that Section 4.1.1 has appropriate applicability specifics, but Section 4.1.2 only says “Transmission Operator”, which initially implies a much greater scope. Request that similar to Section 4.1.1 styling, Section 4.1.2 alternatively state “Transmission Operators notified by a Transmission Owner according to Requirement R3.”

No

Although BHC agrees with the overall approach, it has significant concerns regarding the use of the term “risk assessment” without a clear definition of intent. CIP-002 regulatory expectations in the Western interconnect for RBAM have consistently referred to the classic risk definition as “risk” times “probability”. However, the further expectation is that the probability of an event is assumed to be 100%, such that the “risk” them becomes equal to the “impact”. CIP-014 does not currently lay out the same expectations, which could allow Transmission Owners and other affected (or unaffiliated) parties to disagree over the role of “proabability” in defining risk. This problem can be resolved in the CIP-014 draft by: 1. leaving the risk assessment language as is, but adding the above statements about “probability” of occurrence being 100%, or 2. changing all references of ‘risk assessment’ in the standard, to ‘impact assessment’, or 3. leave the risk assessment language as is, but make it clear that CIP-014 is deviating from the historical CIP-002 RBAM definition of risk, such that the probability

of the event can change the perceived risk (and that such an interpretation is congruent with the FERC order. This last option seems to be closest to the intent of Paragraph 8 in the FERC directive, but represents a significant departure from past NERC CIP guidance, and needs to be highlighted as such. As written, the TO has exclusive determination say in identifying applicable Transmission stations, substations and primary control centers. R2 speaks to a third party verification of that assessment, but Black Hills believes that coordination of the BES would be better served by having the TO & TOP reach a consensus on the assessment, prior to having the assessment validated by a third party. Requirement 2.1 directs the Transmission Owner to select an unaffiliated Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. Firstly, Planning Coordinator does not appear in the NERC functional registry and should not be casually equated with the TP and RC functions; without first equating the Planning Coordinator to the PA function per the NERC glossary. Secondly, none of these NERC functional entity designations appear in the applicability section of the standard. Therefore, it can be assumed that the unaffiliated PC, TP, or RC are not obligated to conduct the assessment themselves, but rather the assessment is conducted by mutual agreement of the TO and unaffiliated PC, TP, or RC acting as third-party assessor. If this is not the correct assumption, then the PC, TP, and RC functions should be noted in the applicability section. If the Transmission Owner is affiliated with the Transmission Planner and Planning Coordinator, then the third-party review should be performed by the entity's Reliability Coordinator. The reference to "primary control center" is adequately explained in the rationale section of R1, but confusion between it and "back-up control centers", "emergency dispatch center", and those control centers that can only monitor status seem to justify an up-front definition in the standard. Recommend that a special definitions section be added, or the term be clearly defined at its first instance in Section 3. R2.4 could benefit from some added guidance regarding the protection of sensitive or confidential information. Is the intent to employ the entity's baseline confidentiality banner, or something more robust such as that required by CIP-003-3 R4 or CIP-011-1. The latter seems more appropriate for this CIP standard.

No

BHC has the same concern with R4 as expressed in the opening comment of the previous section regarding the definition risk assessment. The tailored evaluation required by FERC directive paragraph 8 introduces a probability of less than 100%, which is in conflict with prior NERC guidance on risk definition. As previously noted, if the unique probability of a threat is to be taken into consideration along with the impact, this change from CIP-002-3 expectation should be clearly highlighted. In addition, the inclusion of probability in the risk assessment will increase disagreements between unaffiliated entities, which will require a mechanism for resolution. BHC questions R4.2: The current language states "Prior history or attack". BHC believes this opening should state "Prior history of attack" because the current language does not provide an indication of what 'prior history' is being referred to. BHC agrees with the AZPS suggestion that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions, which would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. BHC believes that the

120 day requirement for R5 should be limited to the development of the security plan, and that full implementation should be dependent on the complexity of the plan. Implementation timing of the entity's plan should be approved by the applicable RC. Provisions could be added for temporarily derating the facility, if the implementation timing were considered by the RC to be excessively long. By mandating a 120 day implementation, entity's security plans may be down-sized to meet the 120 day implementation window, rather than to meet the potential threats and vulnerabilities at the facility. If "implementing" only means the specific deliverables of R5.1, R5.2, R5.3, and R5.4 (i.e. the timeline required by R5.3 is created, but not executed), then "implementation" needs to be more clearly defined. BHC has a further concern that R5.1 language reads too close to the "Identify, Assess, Correct" language already remanded by FERC in the CIP v5 standards. Alternative language for R5.1 might be "Resiliency or security measures designed to prevent potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." This simplification is not expected to change entities efforts, but could be more appealing to FERC. BHC agrees with the reasoning of AZPS to simplify R6.1 to read: "Each Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise." If this language consolidation is not acceptable, then alternatively recommend that Section 6.1.1 be expanded to include other similar certification providers, e.g. the National Sheriffs' Association Institute for Homeland Security offers a Certified homeland protection Professional (CHPP) designation (https://ndpci.us/certification/CHPP_Certifications.php), so as not to appear preferential.
No
Individual
Ayesha Sabouba
Hydro One
Yes
We agree with the Applicablity. R1 has provided flexibility in the assessment method.
Yes
Subsequent risk assessments should be performed every 36 months (to align with CIP requirements) instead of every 30 months. The FERC Order allows for the verification to be completed by NERC, the Regional Entity, an RC or another entity. The standard only identifies that the verification can be completed by a registered Planning Coordinator, Transmission Planner, or Reliabity Coordinator, or an entity with transmission planning and analysis experience; it does not mention NERC or the regional entity.
Yes
The Standard allows the TO and TOP sufficient flexibility to complete R4, R5 and R6.
Yes
Will FERC accept R2.3 and R6.3, which allows the TO or TOP to document why they are not following the recommendations from the verification? The FERC Order did not suggest this. It

is extremely important that all jurisdictions follow the same standard, so that the mitigation of risk to physical security is consistent. Having some jurisdictions who follow a more stringent standard will increase costs to ratepayers in those jurisdictions. The standard should provide a definition for “unaffiliated”.
Group
ERTF
Joe Tarantino
Agree
The following comments are in agreement with LPPC and ERTF as well as comment from our own entity LCRA: • Use of “primary control center” is ambiguous (R1.2 and others); • Unaffiliated third party review needs to be longer than 90-days, suggestion to be 180-days (R2.2); • Issue with non-disclosure agreement vs. Public Power’s obligation to disclose information (R2.4); • Expansion of the Security Plan third-party reviewer to include those functions that are identified in Requirement 2.1 (R6.1). • The standard does not address substations/stations that are owned by multiple Transmission Owners. LCRA TSC recommends adding language describing NERC’s expectations associated with jointly-owned substations/stations or substation/stations with multiple asset owners.
Individual
John Falsey
Invenergy LLC
Agree
NPCC
Individual
David Kiguel
David Kiguel
No
1. For clarity suggest that the word “verify” be changed to “confirm” in sub-requirement 2.2 so that it reads: “The unaffiliated verifying entity shall either confirm the Transmission Owner’s risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). 2. Sub-requirement 3.1 should cover both, addition and removal of elements from the identified facilities list. Suggest changing to: “In the case of addition(s) to, or removal(s) from the identified Transmission stations or Transmission substations list developed under Requirement R1 and verified/modified according to Requirement R2, the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the change(s).”
No

Sub-requirement 6.1.1: While Certified Protection Professional (CPP) or Physical Security Professional (PSP) might be recognized certifications in the U.S.A., that is not necessarily the case across the Canadian Provinces. Recommend to add: “or equivalent in those jurisdictions where such certifications are not recognized.” Sub-requirement 6.4: In addition to the non-disclosure agreements referred to in this sub-requirement, the standard should specify that the reviewing individuals having access to the confidential information must have security clearance and training, similar to the requirement in other CIP standards. Also, the security clearance must be obtained according to the established procedures in the respective jurisdiction.
Yes
The Implementation Plan obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. While performing and completing the vulnerability assessment before the effective date of the standard may constitute a recommended good practice, from a statutory perspective, compliance with the standard before its effective date may not be enforceable in all jurisdictions. An entity cannot be found in violation of the standard at a time when the standard is not yet effective. Recommend changing the implementation plan to require completion of the assessment after the effective date of the standard.
Group
JEA
Tom McElhinney
Agree
APPA
Individual
Michael Haff
Seminole Electric Cooperative, Inc.
National Rural Electric Cooperative Association (NRECA)
Yes
Seminole supports the comments by NRECA. Additionally, Seminole supports the use of CIP-002-5 medium impact criteria for use in CIP-014. CIP-002-5 has at least one issue that will apply to CIP-014 as well. There are multiple ways to interpret the phrase Transmission Facility. One example is clarifying what is in the scope of a Transmission Facility. The definition or other documentation should state that the substation is exclusive of the criticality of any connected substation and clarify that a Transmission Facility as used here does not include Transmission Lines.
Yes
Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. As this standard is based on the same standards as the impact ratings in CIP-002, it would be cleaner to identify any facility that is determined critical under the Assessment with a separate (non-exclusive) impact rating such high physical impact and use this term for applicability for R3-R6. If an entity has a qualified third party perform the R1 assessment on

behalf of or in cooperation with the registered entity, does this also meet the requirement R2? Note that the draft RSAW, not under review here, states that R1 and R2 may occur concurrently. R2.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R1.
Yes
Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. Requirements R4.1, 4.2, and 4.3 should be moved to the guidelines and technical basis as there is excessive flexibility provided to the auditor for concluding whether the evaluation is adequate and potential that an auditor may choose to determine that identification of events was inadequate. R5.2 requiring law enforcement contact information is redundant with EOP-004-2 R1. If an entity has a qualified third party perform the R5 security planning on behalf of or in cooperation with the registered entity, does this also meet the requirement R5? R6.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R
No
Group
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing
Marcus Pelt
Yes
Yes
Yes
Yes
Clarification should be made in the implementation guidance for CIP-014-1 that Verifiers who are also Registered Entities in functions applicable to CIP-014, are not subject to penalty under the requirements of CIP-014 due to verification duties performed at the request of a responsible Transmission Owner and/or Operator.
Group
Arizona Public Service Company
Janet Smith
Yes

See related comments under Requirement 2 below.
Yes
AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications for Requirements 1-3. AZPS suggests that the drafting team modify the term “risk assessment” to “BES impact assessment” in Requirements 1-3. The term risk assessment is not a defined term in the NERC Glossary of Terms. It is used in other CIP standards (CIP-002, and CIP-004) each with a different context. Changing the term to “BES impact assessment” ensures that the risks will be categorized and evaluated correctly. Requirement 2.1 directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. However, none of these NERC functional entity designations appear in the applicability section of the standard. Thus it is assumed that the entities listed above are not obligated to conduct the assessment once selected but rather the assessment is conducted by mutual agreement. AZPS suggests that the drafting team provide clarifying language in the requirement to indicate that the assessment is conducted by mutual agreement between the Transmission Owner and the third-party assessor. AZPS is concerned that the term “primary control center” will be confused with the NERC Glossary Term “Control Center.” The definition of Control Center is partially defined as “monitor and control the BES…”. The rationale for Requirement 1 introduces the term “operationally control” in its definition of primary control center which is further defined to mean “causing direct physical action”. The concept of monitoring is explicitly excluded from this definition. To avoid confusion, AZPS suggests that the drafting team define the term primary control center or adopt a new term that clearly differentiates itself from the common term “control center”.
Yes
AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications or clarifications for Requirements 4-6. AZPS is concerned that Requirement 4.3, which requires the Transmission Owner to evaluate threat warnings from a myriad of sources, will result in inconsistent application by entities. The threat sources need to be consistent, and the threats evaluated must be relevant. AZPS suggests that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions. This would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. Requirement 6 requires Transmission Owners to secure a third-party review of the security plan developed under Requirements 4 and 5. AZPS strongly supports the development of security measures to protect critical substations. However, AZPS believes that requirements 6.1.1 through 6.1.4 add a level of specificity that does not provide an improved reliability benefit and has the potential to create a bottleneck that would make compliance within the short 90-day timeframe very difficult. AZPS contends that the most important quality of the third party reviewer is electric industry physical security expertise. Further, AZPS does not believe that the CPP or PSP certifications provide additional value from a realiability standpoint since neither certification has a sector specific focus. For these reasons AZPS would suggest that 6.1 be simplified to read: “Each

Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise.”
No
Individual
David Jendras
Ameren
Yes
No
(1) Regarding R3 and R3.1, we believe that the 7 day requirement is too short and 30 days would be more appropriate to notify other utilities. (2) R4 should have wording added to the requirement that the R4 evaluation is to be completed 120 days after the completion of R2. Then, the R5 wording should be changed so that the R5 physical security plans should be completed 120 days after the R4 evaluation is completed.
Yes
No
We recommend adding language in the implementation guidance around the application of the terms ‘control center’, ‘primary control center’, and ‘transmission station’ in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies’ ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms. Also, we recommend that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify several questions on the timing of the various implementation stages of the standard, including particularly that security plans are subject to change over time for a broad range of reasons. In addition, we ask the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work.
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes

R1 - It appears the intent of R1 is for a TO (which meets the applicability section 4.1.1) to perform a risk assessment (as defined in the standard) on only those substations that meet the applicability section 4.1.1, not all substations owned by a TO which meets the applicability section 4.1.1 description; however this is not 100% clear. The verbiage of the second sentence in R1 states “The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.” The use of the word “any” in this sentence has led some to believe that a TO (which meets the applicability section 4.1.1 description) will have to assess all of their substations, even those that do not meet the section 4.1.1 description. To address this possible issue, LES recommends replacing the word “any” in R1 with “applicable”. R2 - Smaller TOs may not have the in-house resources to perform the risks assessments required in R1, and may need to contract with a third party to perform these assessments. If the performing third party is not affiliated with the TO, is a second unaffiliated third party verification required as stated in R2? Please revise the requirement to address this situation.
Individual
Gary Kruempel
MidAmerican Energy Holding Company
Yes
MidAmerican Energy Holdings Company (MEHC) agrees with the applicability section.
Yes
MEHC agrees with the R1 through R3 approach. However, MEHC suggests the following changes to improve the standards as written: The term “unafilliated third party” is used in R2 and in R6, but in parts 2.1, 2.3 and 2.3. “unaffiliated verifying entity” and in part 6.3 “unaffiliated reviewing entity” is used. Unless the intent was that the terms have different meanins, it is suggested that “unafilliated third party” be used throughout the standard.
Yes
MEHC agrees with the R4 through R6 approach. However, MEHC suggests the following changes to improve the standards as written: The following rewording of R5 is recommended to clarify that the “build out” of security enhancement schedule. R5 Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator’s primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The plan shall be completed within 120 calendar days following the completion of Requirement R2. Implementation of the plan shall be as documented in the plan.
Yes

1. The standard anticipates the potential for joint responsibility in involving transmission operator control centers for substations identified by transmission owners. It is suggested that additional guidance be provided regarding joint ownership of substations The following addition to the first paragraph under the Requirement R1 heading which is similar to an aswer to this questions in the webinars is suggested: For substations that are jointly owned the owners may jointly designate one of the joint owners to perform the risk assessment for that substation. 2. It is suggested that a clarification be made to the RSAW with regard to the following question: " As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" By referring to risk assessment this seems to imply the stations/substations identified after the completion of the requirement R1 risk assessment rather than just the applicability requirements. It is suggested that the words "as a result of your risk assessment" be deleted from this question. 3. Item 3. in the guidance for Requirement R2 seems to actually be guidance for Requirement R1. However, it does not provide useful guidance for Requirement R1; therefore, it should be removed. The guidance for Requirement R1 that gives the TO discretion to choose its own methods and criteria is preferred. 4. The following modification to one of the sentences in the "Performing Risk Assessment" section of the guidance document is suggested: "Using engineering judgment, the Transmission Owner should develop criteria (e.g. imposing a fault near the removed substation) to identify a contingency resulting in potential widespread instability, uncontrolled separation or Cascading within an Interconnection."
Individual
John Canavan
NorthWestern Energy
Agree
Arizona Public Service, Bureau of Reclamation, Portland General Electric, WECC
Group
Western Electricity Coordinating Council
Steve Rueckert
No
WECC questions why generation assets are exempt from analysis and verification required by Requirements R1 and R2. It is possible that some generation assets, if rendered inoperable, could result in widespread instability, uncontrolled separation, or Cascading. WECC recommends removing the 500 kV line in the Weighted Value table. All 500 kV facilities are to be assessed per Applicability Section 4.1.1.1 and including 500 kV lines in the table in applicability section 4.1.1.2 with a zero value seems more likely to add confusion than to provide clarifying information. Applicability section 4.1.2 makes it look like the standard is applicable to all Transmission Operators. WECC suggests adding some clarifying language to indicate that the standard is only applicable to Transmission Operators notified per Requirement R3. This may serve to make the standard more acceptable to Transmission Operators in general.

No
The periodicity for risk assessments and the forward looking time frame for including planned substations do not match. Entities are only required to consider stations planned in the next 24 months, while the risk assessment is applied on a 30 month cycle, or a 60 month cycle if the entity previously identified a null list of applicable stations. This potentially leaves a 6 to 36 month gap. We would encourage the SDT to match the periodicity of the application to the planned implementation window or include language requiring any new asset be evaluated under R1. WECC notes that the time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. WECC suggests that at a minimum NERC and the Regions engage in extensive outreach to ensure that the Transmission Owners are aware of this and that if possible the drafting team revise the language of Requirement R1 to make this clear. Requirement R2, part 2.2 appears to be assigning responsibilities to the unaffiliated verifying entity (registered Planning Coordinator, Transmission Planner, or Reliability Coordinator) yet these entities are not included in the applicability section. If these entities are to be held accountable in the standard for actions, why are they not included in the applicability section?
No
From a compliance perspective, WECC notes that the criterion identified in R4 is too vague to enable a consistent approach across regions or even entities. Identifying a basic set of attack vectors that must be considered (ie: direct fire ballistic attack, indirect fire attack, explosive device attack, vehicle-borne attack, arson/incendiary attack) fosters a far more consistent approach while allowing the entity the flexibility to tailor their assessment and security plan to the unique characteristics and threat landscape of their asset(s). WECC is concerned that the language of Requirement R5 is confusing or contratictory. Requirement R5 requires the applicable entity to “develop and implement” a documented physical security plan…within 120 calendar days following the completion of Requirement R2. However, part 5.3 requires a timeline for “implementing” the physical security enhancements and modifications specified in the physical security plan. WECC questions whether Requirement R5 requires the physical security plan to be “developed” or “developed and implemented” within 120 calendar days following the completion of Requirement R2. If Requirement R5 requires “development and implementation” within 120 calendar days following the completion of Requirement R2, what is the purpose of the timeline for implementing the physical security enhancements and modifications specified in the physical security plan required by part 5.3?
Yes
WECC believes that the proposed standard addresses the FERC Order and has voted affirmative to approve CIP-014-1. However, as noted in our comments above we believe there is opportunity for enhancements and clarification that if implemented would improve the standard and still meet the FERC Order. WECC encourages the drafting team to consider implementation of these suggestions prior to the final ballot or NERC to submit a SAR for consideration of these suggestions immediately after approval of the standard.
Group

NCPA Compliance Management Operating Committee
Steve Hill
No
The Standard Drafting Team (SDT) estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability or uncontrolled separation. The Applicability section creates a lot of work for many TOs an TOPS to identity those 30 or less transmission stations out of the 55,000 substations. The SDT might consider a higher level of applicability as was done for EOP-010-1, Geomagnetic Disturbance Operations i.e. apply the standard to Reliability Coordinators (RC) and only the Transmission Operators the RCs deem critical.This would be a more efficeint filtering process. Benefits of such an approach would be (1)Simplification and tighter security of critical information and informaton sharing (2) streamling and simplicaton of requirements for unaffiliated third party review, for example one reviewer could handle the risk assessment, vulnerability and threat assessment and review of security plans (combines requirements R2 & R6 together) (3)Time and resources of the entity could be more efficiently and economically managed as all reviews could be handled by a single Reviewer in a continuous manner rather than starting a stopping for different phases. (4) Saves many entities who would fall out of the process after going through the first three requirements. I expect RCs, ISOs and Regional Entities already know this
No
Applicability is a key issue here. Comments to question 1 apply here as well. Why subject all Transmission Owners who may meet the "medium impact under CIP-002-5.1 to a third pary review for all medium impact stations and substations when only 30 stations will be affected (please define the difference between a Transmission station and Transmission substation. A third party review is appropriate for the 30 or so stations involved, but seems excessive for all owners to obtain third party review when the expectation is that 30 out of 55,000 are te ones of real concern. NCPA elected to have an independent third party risk asssessment and vulnerability assessment performed at its 5 generation facilities and control center. The assessment cost is approximately $150K and takes about 9 months to complete. NCPA'a assets are also low impact. The risk assessment, vulnerability and threat assessments and development of the security plans are able to performed by the same third party reviewer that flows together without interruption. The way in which the requirements are structured creates alot of consultants or third party reviewers running around, with 99% of them stopping work after R3. How much money will be spend for that and for what purpose? There has to be a better way segregate the 99% from the 1% where the real concern is.
No
Same line of reasoning as given in the response to the question 2. If the Applicability Section were changed R1, R3, R4,and R5 could be combined together and R2 and R6 could be combined together. This simplifies the standard and gets to the heart of the Reliability

Concern without creating a Consulting industry to perform third party reviews. (If you don't like the suggestion, maybe I found a new business opportunity)
Yes
The Implementation Plan is too agressive. I cite NCPA experience as described in our response to question 2. I find it interesting the the CIP-version 5 standards have essentially a two year implementation plan for medium and high assets and yet this proposed standard has a 6 month implementation plan.
Individual
Joe O'Brien
NIPSCO
In R2 we are not sure who would do the verification. On one of the webinars a member of PJM suggested that another PJM member could be a candidate. However it is likely that a PJM member is not a PC, TP or RC as prescribed in the requirement; that role is performed by PJM itself. Any further guidance would be welcome; we do not consider this a "show stopper". The hard work that went into putting this project together in such a short time frame is appreciated, thanks.
Individual
Wayne Sipperly
New York Power Authority
Agree
APPA
Individual
Megan Wagner
Westar Energy
Yes
No
The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time.” While not specifically

referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments.
Yes
Yes
Effective Date: The use of the term 'implement' needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs: Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2. Insert 'and verified according to Requirement 2' following the reference to Requirement R1 in all the VSLs for R5. Delete 'and modify or' in the last High VSL for R6. Guidelines and Technical Basis: Replace 'drafting team' with 'SDT' in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6. Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary. Insert 'Transmission', capitalize 'Owner' and delete 'or operator' in the 1st paragraph under Requirement R2 on Page 29. Make 'outage' plural in Bullet c. at the top of Page 30. Capitalize 'Transmission Owner' in the 4th bullet in the middle of Page 30. Capitalize 'Owner' in the 1st line of the paragraph immediately preceeding Requirement R3. Insert 'Requirement' in front of R5 in the last line of the paragraph immediately preceeding Requirement R6. Spell out TO and TOP throughout the document. RSAW: The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states '…any risk assessments conducted prior to the effective date of this standard are not relevant…' is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there 'This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.' We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states "The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard." Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective. Replace 'with' with 'within' in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2. Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4. The phrase 'and compensating mitigating measures' in the 4th row in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Individual

Amy Casuscelli
Xcel Energy
Yes
Yes
Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team. R1 requires an assessment of facilities, including those to be in service within the next 24 months, followed by an additional review every 30 or 60 months. If a facility is brought into service, it is unclear when the review should be performed due to the 6 month gap between the in service date and the review. R2 requires a Transmission Owner to have an unaffiliated third party "verify" the risk assessment performed under R1. By contrast, R6 requires each Transmission Owner to have an unaffiliated entity "review" the evaluation performed under R4 and the security plan under R5. Xcel Energy recognizes that use of "verify" and "review" reflects the Commission's wording, but it would be helpful if the standard explained the difference between the two terms, if there is a difference. The 90 days prescribed by R2 to obtain third party verification may be too restrictive due to the availability and/or capacity of applicable resources. The standard requirement which imposes the action/deliverable by a third party, but the accountability to the TO/TOP, is also a cause for concern. It might be better to have the timing of R1 and R2 combined as this would enable flexibility of performing the assessment and completing the third party verification within the overall timeframe desired. We also suggest the Regional Entities or NERC be considered as parties that can provide third party verification and contract out if desired. It would also be helpful to expressly clarify in R2.1 that an "entity with transmission planning or analysis experience" could include a peer TO/TOP or a panel of employees from peer TO/TOPs, for example from the North American Transmission Forum. Allowing peer review would assist in identification and dissemination of best practices, we believe. R2.3 requires documentation of any recommendation to add or remove facilities as recommended by the verifying entity, but does not specify if any actions are required if no recommendations are made. Since the VRFs reference various levels of severity based upon documentation of recommendations, it would seem beneficial to allow a "no recommendations" option. Also, it is unclear if there are specific criteria the third party reviewer should utilize to review/verify and make recommendations if facilities are to be added or removed. While an entity could indicate why recommendations were or were not adopted, it would be useful to have verification criteria defined more clearly. R3 seems to be unclear in whether TOs or TOPs have operational control over facilities. In order to more clearly identify that TOPs have operational control, R3 should indicate that the TO shall notify the TOP of the identified facility.
Yes
Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team. The rational for R4 and R5.1 indicate that there is no required timeframe to complete the evaluation of the potential threats and

vulnerabilities to identified facilities, but it does indicate the linkage of completing this when the physical security plan developed as part of R5 and within 120 days of completion of R2. We suggest that it might be more efficient to combine R4 and R5 or clearly show the linkage to reduce confusion about the timing of these two activities. Maybe the standard should require entities to develop a physical security plan after the risk assessment is completed, not after a verification of facilities as specified in R2. If R2 returns a null set, this seems ambiguous as we may still be required to have a physical security plan, even if blank. Since R4 would only be considered applicable if the R2 risk assessment process identifies facilities, referencing R4 in R5 would seem more intuitive. R5.2 states that the physical security plan must include law enforcement's contact and coordination information. However, guidance on law enforcement and coordination has already been established with the adoption of EOP-004-2. It is also unclear by what is meant by "coordination". Since reporting a physical threat to a Facility is a requirement of EOP-004-2 and in order to remove ambiguity around the word coordination, we propose changing R5.2 to read "notification of law enforcement consistent with EOP-004-2". This would avoid potential confusion whether the R5.2 requirement is different than the EOP-004-2 requirement. R6.1, While there will be some regional variances, if an entity spans multiple regions or even some governmental agency jurisdictions, what protection does an entity have against reviewer discrepancies or differences? For example, the Xcel Energy registered entities anticipate using a common risk assessment methodology, and similar security plans. It would be efficient to have a single evaluator provide the review for all three Xcel Energy registered entities. It would also be important for Regional Entities to apply consistent criteria when auditing the risk assessments and security plans. R6.1.2, if the ERO does not meet any or some parts of the criteria established in R6.1, it is uncertain how the ERO will be able to determine and approve an organization that does. Our security department, like the departments at other utilities of similar size, consists of a mix of multiple CPP and/or PSP holders, prior law enforcement professionals and several career military experts, including nuclear military asset security. It would seem that resources within the industry are the most knowledgeable resources available to evaluate physical security plans, given the criteria, and would have more utility specific knowledge than outside entities. Similar to our comments regarding R2.1, since the industry has the most knowledge on threats and vulnerabilities, and means to prevent them, we again propose adding an option to allow for industry (but non-affiliated) peer review of the physical security evaluation, either directly or through a group organization such as the North American Transmission Forum. Allowing peer review is likely to assist in identifying and disseminating best practices, thereby improving security. R6.3. Similar to our comments regarding R2.3, if no recommendations are made for changes to the evaluation by the unaffiliated reviewing entity, does this conclusion need be documented? Since some of VRFs are built off this requirement, it would seem to follow that all aspects be included to ensure certainty for the industry.

Yes

Since existing criteria from CIP-002-5.1 is used to identify facilities in scope, Xcel Energy suggests the addition of the proposed requirements be incorporated to CIP-006-5 (rather than in an entirely new standard) to more closely align and standardize the oversight of R3 and R6. In addition, this would centralize all physical security requirements within a single

Standard. Additionally, there is a significant amount of language in the requirements to specify the affected parties. We suggest the Standard Drafting Team seek opportunities to more concisely outline the applicability and the subsequent obligations in the requirements, to improve ease of understanding. We see an opportunity for the audit or risk functions of the Regional Entities to align with the third party review criteria established in the proposed standard. Although the expertise to perform this function may not currently be in place, the Regional Entities could easily develop the knowledge and expertise, and the reviews could naturally integrate within their other review and assessment activities. Overall, the standard is very comprehensive as drafted and it is balanced in a manner that allows for maximum flexibility. Consistent with NERC's evolution to results-based standards, it is appropriate for the standard to focus on the desired results of increased security of critical facilities, rather than mandating rigid actions that may or may not be suitable for individual facilities and entities. Allowing industry the latitude to design its own mitigating measures ensures those measures will be the most practical and cost effective as appropriate for the particular nature of each facility. The flexibility of this proposed standard is the best opportunity for the industry to execute a comprehensive solution based on assessments and security that relies on the unique design and characteristics of the operating systems of each utility.
Individual
Mahmood Safi
Omaha Public Power District
No
The Omaha Public Power District (OPPD), suggests replacing the term "primary control center", using the NERC defined term "Control Center", with "primary Control Center".
No
OPPD, in general, is in agreement with the approach taken in CIP-014-1 for identifying critical Transmssion stations and substations. We agree that risk assessment be conducted using transmission planning analysis, however, we suggest that this standard identifies what applicable planning analysis is used. We think the TPL standards provide the ability for the Transmission Owners to determine the worst case extreme event for identifying critical transmission stations and substations. OPPD believes that leaving R1 open and vague would encourage various interpretations of the term 'transmission planning analysis' as it applies to a 'risk assessment'. This may place the industry and the ERO in the same position as they were with the ealier versions of CIP-002 and the associated RBAM. Referencing the applicable TPL standards attemptes to remove some of this ambiguity by providing a more concise framework to evaluate those worst case extreme events. Furthermore, since TPL standards associated transmission planning analyses are performed in coordination with the PCs, risk assessment verification by PCs/RCs will not require a re-assessment of a study that has already been performed. We suggest that the SDT consider specifically defining 'transmission planning analysis' to avoid repeat of the uncertainty and vagueness associated with the CIP-002 RBAM. OPPD asks the SDT to consider revising requirement R1 as following: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments

of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The transmission planning analysis shall be based on the applicable portion(s) of the TPL standards and specifically referenced. [VRF: High; Time-Horizon: Long-term Planning] 1.1. Subsequent risk assessments shall be performed: • At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or • At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. 1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.
Yes
Yes
OPPD believes that the third-party verifications in requirements R2 and R6, to be performed once every 60 calendar months, not each time when a risk assessment analysis or security plan is changed that does not significantly change the facilities identified or the associated security plan. The transmission entity can still perform analysis and update security plan accordingly as required by this standard, however, the third-party verification should be reserved for major changes to the assessment or the plan or otherwise be done every 60 calender months.
Individual
Bruce Metruck
New York Power Authority
Agree
APPA
Individual
Russell Noble
Public Utitliy District No. 1 of Cowlitz County, WA
American Public Power Association
No

We strongly disagree with applicability statements being outlined in the requirement. We support APPA's recommendation to further define TOP applicability in section 4.1.2 to avoid nuisance compliance certifications.
Yes
However, the TOP does not receive any relief from R1-R2 null set(s) and will be required to provide attestations to auditors and yearly certification of the absence of any notice from Transmission Owners.
No
We are very concerned with the preferential endorsement this Standard affords to ASIS International. We know of at least one other security organization that offers a security certification: the Certified Homeland Protection Professional (CHPP) designation form the National Sheriffs' Association Institute for Homeland Security. If this requirement is left unchanged, FERC's statutory obligation in determining a proposed reliability standard is "not unduly discriminatory or preferential" may trigger the standard to be remanded back to NERC. It is for this concern, and only this concern Cowlitz votes negative. However, Cowlitz plans to vote affirmative in the final Ballot, regardless of any concerns to allow NERC to meet FERC requirements.
Yes
Cowlitz commends the SDT's effort in a very difficult situation.
Individual
Dennis Minton
Florida Keys Electric Cooperative
No
• Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is FKEC’s understanding that a “station” equates to a switchyard that does not include transformers; and a “substation” is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. • Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
No
• Comments: R1.1 – FKEC recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straight forward than a 2.5 year focus and it’s easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. • R2 – The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word “should,” not “shall” or “require.” The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what “verify” means in the standard.

Guidance and rationale is helpful, but does not carry to legal weight of the standard language. • R2.1 – This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. o Are there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in theNERC facility ratings alert responses. o How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. o If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired – this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. • R2.2 – This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. • R2.4 – The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity • R3.1 – The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. FKEC believes 30 days is more appropriate timeframe for this requirement.

No

• It's unclear how an auditor will judge compliance with R4 and its subrequirementsas it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. • R5.1 – FKEC strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement and resiliency will be next to impossible to audit. • 5.3 – After the word "modifications " add ",if any," as this is a possibile outcome. • R6 – Same as comments on R2 in Question 2 above. and R2.1. • R6.1.1 – NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides

for the necessary skills under this standard. • R6.1.2 – It is highly unlikely that the ERO is not going to approve consultants for industry use. This should be removed. • R6.1.3 – All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. • R6.1.4 – It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Yes
Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.
Individual
Bill fowler
City of Tallahassee
Agree
APPA
Individual
Chris Scanlon
Exelon
Yes
Yes
R2.1 Drafting Team could consider adding a note to R2 Guidance section similar to that which is included in the recently approved MOD-032 standard. "Planning Authority and Planning Coordinator" (hereafter collectively referred to as "Planning Coordinator")combines "Planning Authority" with "Planning Coordinator" in the list of applicable functional entities. The NERC Functional Model lists "Planning Coordinator" while the registration criteria lists "Planning Authority" and they are not yet synchronized. Until that occurs, the proposed standard applies to both Planning Authority and Planning Coordinator."
Yes
No
Individual
Linda Jacobson-Quinn
FEUS
Agree
APPA WECC

Individual
Dean Ahlsten
Eugene Water & Electric Board
Agree
American Public Power Association (APPA)
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
Yes
No
Do not support the third party requirements, seems like a full employment effort by security consultants and others. Administratively burdensome and time-consuming at the expense of actual security improvements.
No
Again, do not support the third party review requirements. Already an auditable standard approach.
No
Individual
Steven Wickel
Public Utility District No. 1 of Chelan County
Agree
LPPC and APPA
Individual
John Yale
Public Utility District No. 1 of Chelan County
Agree
LPPC and APPA
Individual
Hugh Owen
Public Utility District No. 1 of Chelan County
Agree
APPA and LPPC comments
Group
Con Edison and Orange & Rockland
Peter Yost

No
Reliability Coordinator, Planning Coordinator and Transmission Planner should be added to the Applicability Section. That will obligate these entities to meet the 90 day review period stipulated in R2.2, if they are identified as a verifying entity by the Transmission Owner.
Yes
Yes
Yes
Section: Purpose Comment: Use of term “primary control center” should be clarified. If an entity has a primary control center and a redundant back up control center, is the back up control center also in scope for CIP-014? Requirement 1: is the intent of the Standard that the R1 risk assessment be applied to transmission stations or substations identified under Applicability 4.1.1.4, as meeting NPIRs? Requirement 4: If under Requirement R4 a Transmission Owner owns or operates a single substation that employs multiple voltage levels, then which portions of that substation would be covered by CIP-014-1 and the Entity’s physical security plan, and which would not be covered? Requirement 5: Consideration of transmission system “resiliency” is more appropriate to be applied during the R1 risk assessment, as opposed to the R5 physical security plan. Recommend moving references to resiliency to R1.
Individual
Mike Marshall
Idaho Power Co.
Yes
4.1.2. Seems vague in its description lending the reader to believe that TOPs are in scope at all times which is inconsistent with guidance later in the standard which states they are only required to perform actions when informed they are in scope by a TO. Further Clarification is needed in this section.
Yes
Further clarification is needed on several points. There is no specificity to provide consistency with how the "risk assessment" should be performed or what methodology or components to the methodology should be used. Additionally, there is no defined meaning of "widespread instability, uncontrolled separation, or Cascading within an Interconnection." Does this refer to regionally identified IROLs or some other objective criteria or only based on the analysis performed? Additionally, there is no mechanism built into R3 to allow for a dispute between a TO and a TOP if they disagree on a particular station or substation as there is in the third party reviews under R2 and R6 where there is a mechanism to disagree with the reviewer.
Yes

Further clarification is needed on several points. 4.2 & 4.3 leave open much room for interpretation under audit to say you did or didn't consider a particular source or threat. There is also some consternation over the use of "potential threat" in this requirement. There are a great many potential threats many that are so remote and nearly impossible to protect against that the risk does not outweigh the cost. It seems like these sub-requirements are a potential audit findings trap by the way they are worded. There are also no criteria specified for what the unaffiliated third party will be looking for in their review of the entity's evaluation. There is a great deal of concern for how these third parties will be able to handle or be willing to handle the influx of these reviews especially considering the short 90 day timeframe listed in 6.2.
Yes
There is great concern related to information protection related to turning over information concerning vulnerabilities of the grid and related facilities to outside parties. Even with the use of NDAs, these third parties are not subject to the same NERC reliability standards (i.e. CIP standards, information protection, etc) as the entities, will not be audited on their information protection practices, and may have no accountability to the regulators in the event of a disclosure of sensitive information, inadvertent or otherwise. It is a concern that the TO is responsible for 3rd party verification to be completed within a tight 90 day window, especially considering the critical infrastructure information being exchanged. Contractual exchanges and negotiations could impede upon the 90 day window. Also, TO's may need time to review the R2 study results and possibly mitigate study discrepancies. The date R1 needs to be performed is unclear. Does it need to be performed within a certain amount of time after the effective date? The implementation plan states that the initial risk assessment must be performed on or before the effective date of the standard. However, the RSAW for R1 states that "any risk assessments conducted prior to the effective date of this standard are not relevant." Does this mean the initial risk assessment must be performed “on” the actual effective date of the standard? Is there a basis for the short notification window in R3? The seven calendar days window for the TO to notify the TOP seems quite short. Additionally, there is a discrepancy in the review timeframes in R1 in which a look ahead of 24 months is required for stations and substations that are in the planning process but the risk assessments are performed every 30 months leaving a 6 month gap in the analysis. It would also seem more intuitive and consistent with other CIP standards to have the risk assessment requirement performed on an even year rather than a 30 month basis (i.e. 36 months.)
Individual
Chad Bowman
CHPD
Agree
CHPD is supportive of the comments submitted by APPA
Group
ACES Standards Collaborators
Ben Engelby

Yes
We support a clear and defined “bright line” criteria that has been industry vetted and FERC approved as the starting point for the risk assessment in R1.
No
(1) Conceptually, we agree with this approach but have identified the following issues and concerns. (2) R1 requires additional clarification. The Guidelines and Technical Basis section states that the “bright line” criteria in applicability section is used to identify an initial set of stations and substations that must be further evaluated in R1. It is our understanding that if a TO owns one 500 kV transmission station and no other transmission facilities, then that 500 kV station would meet the applicability section 4.1.1.1 criteria. The TO would be required to perform a risk assessment to identify if that facility was rendered inoperable, it could result in widespread instability, uncontrolled separation, or Cascading in an Interconnection. In other words, if the applicability section is met, the TO must perform a risk assessment, but the remainder of the standard (R4-R6) would not apply unless loss of the Facility would result in widespread instability, uncontrolled separation or Cascading. Please confirm if our understanding of applying the requirements is the correct approach. (3) We see a significant compliance risk created by Requirement R2 and question why the unafilliated third party verification cannot be integrated into the Regional Entity compliance monitoring and enforcement processes to minimize costs and limit access to highly sensitive information. The third party verification creates a compliance problem outside of the TO’s control because the TO is dependent on a third-party for regulatory compliance and there is no obligation on any of the third parties (i.e. RC, PC) identified in the standard to verify the risk assessment. Thus, the TO will have to rely on consultants to perform the verification. Since all TOs will be working towards the same efffective date, there will be a backlog and the reviews may not be completed by the timelines established in the standard. Review by consultants also will increase the number of people with access to highly sensitive information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. All of these issues could be resolved if NERC and Regional Entities conducted the review. The review could be performed as part of a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolved the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. As an alternative, we suggest that a companion requirement that compels either the RC or PC to perform the verification. This would also reduce the costs impacts and distribution of sensitive information since these entities will already be familiar with the TOs they are verifying and will already have access to highly sensitive information. (4) Regarding R3, this requirement does not warrant a 7-day timeline. This is not a near real-time issue. We suggest 30 days as a reasonable notification period.
No

(1) We see a significant risk of the compromise of highly sensitive information created by Requirement R6 and question why the unaffiliated third party review cannot be integrated into the ERO compliance monitoring and enforcement processes. There is no compliance obligation on these third parties to complete the review within the required timelines, which could subject the TO to potential compliance violations. Furthermore, there is a limited set of companies with qualified personnel capable of performing this review. Given that all of the Transmission Owners will be working toward the same effective date of the standard, it is highly likely that a backlog of work would occur. Furthermore, review of the evaluations by consultants will increase the the number of people with access to higly senstivie information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. To resolve this inssue, NERC and Regional Entities could hire qualified personnel to perform these reviews. NERC and Regional Entities could perform a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolve the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. (2) How can the 'cost to benefit to risk to the BES' be measured consistently across each facility, region and risk? Does a Registered Entity have to authority to not implement a 'recommendation' from a third party based upon a cost to benefit to risk analysis? (3) Given that third parties are required to evaluate critical facility information, further guidance is needed for the required controls to prevent unintended release of highly sensitive and confidential information. What is the risk to the Registered Entity if the information does get leaked? Is this a violation to the Registered Entity, even if the leaked information was not caused by the Registered Entity? We are concerned that if this information were to be leaked, the Registered Entity could be liable for increased risk of attack, additional time and costs to address the leak and could impact the BES due to changes in operations from shutting down those facilities. (4) Part 4.2 has a potential "prove the negative" issue. How do you prove that you considered similar facilities particularly when similar facilities could includes other company's facilities. To resolve this issue we suggest replacing "similar" with "nearby facilities" or "asset owner's other facilities in the area". (5) Part 4.3 could be interpreted as requiring consideration of all threat and intelligence information including information that is not relevant to a given area. To remedy this issue, we recommend using the term "current and local" to describe the types of intelligence and threats that must be considered. (6) We believe that Part 5.2 is redundant to the EOP-004-2 – Event Reporting, especially Attachment 2 Event Reporting Form line 4. Please consider removing and comparing the standard in its entirety to EOP-004-2 to avoid unnecessary duplication. (7) For Part 5.4, please modify the language to clarify that it only applies to facilities identified as a result of application of Requirements R1 and R2. (8) For Part 6.1 please modify "… from the following" to "… from one of the following". This will make it perfectly clear that only one entity must be selected.
No

Thank you for your time and consideration.
Individual
David Thorne
Pepco Holdings Inc.
Yes
Yes
Yes
Yes
There seems to be a conflict between the RSAW, Consideration of Issues or Directives and the Timeline included in the FAQ. To meet the overall timeline for the entire standard, the risk assessment must be started prior to the Effective date of the standard. There should be no prohibition for completion of the Risk Assessment prior to the Effective date of the standard. The FAQ Timeline states: “Initial performance of R1 must be complete on or before the effective date of the standard…” The Consideration of Issues or Directives #12: “…This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard…” The RSAW under R1 Evidence Requested states: “Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant).”
Group
American Public Power Association (APPA)
Allen Mosher
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. CONTROL CENTER - Use the defined term “Control Center” by capitalizing as “primary Control Center” or explain why lower case “primary control center” is different and needs to be used in the standard. Consider inserting “with operational control” after primary Control Center, to express the intent of the text box Rationale for Requirement R1 that the control center must be capable of taking electronic actions that can cause direct physical actions at the identified station or substation. Please also clarify whether the periodic use of a

backup control center as the entity's primary control center would make R4 and R5 applicable to both the primary and backup control centers. UNAFFILIATED - needs to be either defined or a footnote needs to be added to the standard to explain that "unaffiliated means that the selected verifying or reviewing entity cannot be a corporate affiliate," as stated in the guidance section. CONFIDENTIALITY Publicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS: R1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3.2 The Transmission Owner will keep confidential all records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard. R4.4 The Transmission Owner and each applicable Transmission Operator will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1. APPA suggests technical edits to Requirements R2.4 and R6.4 to insert "or made available to" after "exchanged with." This change would clarify that sensitive or confidential information does not have to be actively "exchanged" between entities to be subject to the protections directed under Requirements R2.4 and R6.4. APPLICABILITY 4.1.2 - The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would

be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective: 4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3. Please also confirm that the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. TIMELINES to complete third party verification under R2 and third part review under R6 are both too short. Increase 90 days to 120 days or 180 days. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A short 90-day time limit may not be sufficient time to conduct and verify a revised or supplemental BES assessment. For security reviews, conducting a meaningful review with sound recommendations applicable to a specific TO's or TOP's facts and circumstances may also take time along with necessary discussions with the TO. A short review window is more likely to lead to disagreements with the TO which in turn would lead to discrepancies that would need to be justified – which in turn might cause the reviewer to avoid making proposals that should be considered by the TO or pressure on the TO to accept recommendations that could be improved upon. R1 GUIDANCE - TRANSMISSION PLANNING BASE CASES: Please revise the Guidance for R1 to clarify that TOs should start their initial and subsequent risk assessments with a common regional or area transmission planning base case used for transmission planning purposes. The base case should include existing BES stations and substations and those planned to be in service within 24 months within the region or area, to ensure forward-looking risk assessments and security planning. R2 VERIFICATION - Third party verification of third party risk assessments conducted under R1: some medium sized TOs with applicable transmission stations and substations may contract with a third party consultant to conduct necessary BES risk assessments, to ensure accurate and comprehensive consideration of the risk of widespread cascading, instability and uncontrolled separation. Such entities seek clarification that a single expert risk assessment study, in conjunction with a verification by an unaffiliated PC, TP or RC would suffice.
Yes
APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. R4 CLARITY - Under R4, combining the applicability of this requirement to both TOs and TOPs with applicable control centers within a single sentence is confusing and could be read to imply that a TOP that is affiliated with a TO must arrange for a separate third party review. We recommend revising R4 to read as follows: R4 Each Transmission Owner that

owns a Transmission station or Transmission substation identified in Requirement R1 and verified according to Requirement R2, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s) and Transmission substation(s), identified in Requirement R1 and verified according to Requirement R2. Each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to their primary control center identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning] R4.2 TYPO – Please change: "Prior history or attack..." to "Prior history OF attack..." Make conforming edits to the RSAW. 30-MONTH CYCLE - Identification of new threats and vulnerabilities in R5.4 does not change the 30-month cycle for conducting reliability studies and security evaluations: The standard needs to make clear that the security plan needs to take into account threats and vulnerabilities that are known at the time the plan is developed and the approved plan is capable of addressing new threats and vulnerabilities as they emerge, but that there is no NERC requirement to revise the plan between 30 month cycles and for the NERC CEA to audit such revisions. The TO should apply its existing security plans and procedures to evaluate and mitigate evolving security threats. The TO may also revise the security plan in mid-cycle if it so chooses without arranging for a third party review, but that action does not obviate its obligation to conduct the "subsequent" risk assessment and threat evaluation and security plan on the 30 month cycle. The CEA will audit the processes the TO uses to develop its plans, rather than the content of the plans. REQUIREMENT R5 CLARITY – R5 states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." Please change "implement" to "complete." The use of implement can easily be read to require the actual implementation of physical security measures within 120 days, rather than the completion of the security plan, starting the 90 day clock for unaffiliated third party review under R6. In contrast, R6 states that: "The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5."

Yes

APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members. See comments on definitions under Question 1. RSAW for R1 poses the following question: "As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" This question combines a multi-step process into a single question that cannot be answered as yes or no by many TOs. Please break the RSAW for R1

into three discrete questions: 1…Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1? 2…Have you conducted a risk assessment of each applicable station or substation identified under Applicability section 4.1.1.? 3…Did the risk assessment identify one or more Transmission station(s) and/or Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? RSAW R1 evidence request text from near the top of page 6: (R1) Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant). The draft Implementation Plan states that the risk assessment required by R1 "must be completed on or before the effective date of the standard," yet the RSAW language provided above seems to exclude such an assessment. RSAW R1 "Note to Auditor" on page 7: “Review entity’s answer to the above Question and if the auditor can verify the answer is ‘no,’ Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary.” The text appears to reference the following question from page 6: “As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?” This question is poorly worded, because TOs not meeting the applicability requirements of 4.1.1 are effectively exempt from this standard and do not need to perform a risk assessment. RSAW R3 "Question" on page 11: Please reword to add the following all caps text: “Are THERE any primary control centers identified in Requirement R1, Part 1.2 THAT ARE not under operational control of your NERC registration? RSAW R4 "Compliance Assessment Approach" on page 14: Change “or” to “OF” (R4 Part 4.2) “Prior history OF attack...” See the language used in the Guidelines and Technical Basis on page 31 of the standard. RSAW R5 "Note to Auditor" on page 16 states: “Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities that would facilitate physical attacks that have a high probability or likelihood of occurrence.” The requirements of the standard do not address "probability" or "likelihood" of occurrence, so these factors should not be in scope of the compliance audit. Rather, auditors should address whether the security plan is complete and the TO or TOP addresses the issues raised by the third-party reviewer.
Individual
Melissa Kurtz
US Army Corps of Engineers
Agree
Western Area Power Administration
Individual
Shirley Mayadewi
Manitoba Hydro

Yes
Yes
No
(1) Manitoba Hydro has concerns about the need to have a third party to review or verify risk assessments and physical security plans. It is unclear at this point what measures or counter measures are being alluded to here as far as protecting critical assets such as lines and towers. This may potentially be financially burdensome as well as questionably effective. (2) Also missing in the standard is conflict resolution between a TO and this third party reviewer. Clarification should be provided on who weighs in on this and how NERC audits a system that has been verified by a third party. As currently drafted it appears that the third party reviewer/verifier would have no liability under the standard.
Yes
(1) R6.1 – It is not clear whether only one or all of the qualifications in Section 6.1.1 through 6.1.4 must be met. Accordingly, R6.1 should be rephrased to refer to “one of the following”.
Individual
Debra Warner
self
No
While the reqirement for unafflilated third party verification of the security plan is required by the FERC order, I believe the mandate will lead to future security compromises.
Group
FirstEnergy
Doug Hohlbaugh
Yes
Yes
FirstEnergy supports the proposed requirements R1 through R3.
Yes
FirstEnergy supports the proposed requirements R4 through R6 but offers two comments: 1) In regard to the inclusion of “primary control centers,” we suggest the team add language within the Guidelines and Technical Basis section for requirement R4 and potentially the inclusion of an additional FAQ item to document some of the team’s feedback provided

during the webinar sessions. During the webinar the team provided a good explanation of how CIP-014 is uniquely different than physical protections provided under CIP-006 and that CIP-014 provides perimeter protection of the primary control center location or site and not just the subset of the control center that may house cyber assets protected under CIP-006. 2) Regarding requirement R5, during the industry webinars it became evident that there is some confusion associated with the word “implement” as used in the statement “shall develop and implement a documented security plan(s)” and that some industry stakeholders questioned if implement intended completion of all identified tasks stated within the plan(s). While FirstEnergy understood the requirement as described by the team during the webinars, to alleviate any confusion and better clarify the intended application, FirstEnergy suggests changing “implement” to “initiate” or “issue” so that it reads “shall develop and initiate a documented security plan(s)”. This wording may better align with part 5.3 and the guidance provided in the Guidelines and Technical Basis section that states “Entities have the flexibility to prioritize the implementation of the various resiliency or security measures in their security plan according to risk, resources, or other factors.”
No
FirstEnergy supports the proposed standard and appreciates the teams consideration of our comments intended to help clarify a few areas of the standard. FirstEnergy appreciates the team’s efforts in producing a quality standard within an expeditious schedule and believes the team has provided a product that meets the core expectations described by the FERC Order.
Group
Seattle City Light
Paul Haase
Yes
Seattle City Light supports the Question 1 comments of APPA, with one exception in the area of Confidentiality. Seattle's comments about Confidentiality, in place of APPA's comments on this topic, follow. CONFIDENTIALITY The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be

kept confidential by the owner of the records and information, those entities with authorized access to the records and information, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language: R1.3 Records and information related to the risk assessments conducted under this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R3.2 Records and information related to the risk assessments conducted under Requirement R1 of this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R4.4 Records and information related to the evaluation of physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and/or Control Center(s) identified in Requirement R1 conducted under this standard that are designated confidential by the Transmission Owner or Transmission Operator are [intended to be] exempt from public disclosure.

Yes

Seattle City Light supports the Question 2 comments of APPA as well as the additional comments of Salt River Project (SRP) regarding 3rd party verification. Third Party Verifiers (SRP): SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or

fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Yes
Seattle City Light supports the Question 3 comments of APPA.
Yes
Seattle City Light supports the Question 4 comments of APPA.
Group
SPP Standards Review Group
Robert Rhodes
No
We have some concern with the undefined term ‘collector bus facility’. Without a definition for collector bus facility some may consider the entire switchyard at a generating station as a collector bus facility. We do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
No
The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate

confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time.” While not specifically referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments. We strongly suggest that the SDT expand on this addition to R1 in the guidance document to provide needed clarification to the industry.
Yes
Yes
Effective Date: The use of the term ‘implement’ needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs: Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2. Insert ‘and verified according to Requirement 2’ following the reference to Requirement R1 in all the VSLs for R5. Delete ‘and modify or’ in the last High VSL for R6. Guidelines and Technical Basis: Replace ‘drafting team’ with ‘SDT’ in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6. Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary. Insert ‘Transmission’, capitalize ‘Owner’ and delete ‘or operator’ in the 1st paragraph under Requirement R2 on Page 29. Make ‘outage’ plural in Bullet c. at the top of Page 30. Capitalize ‘Transmission Owner’ in the 4th bullet in the middle of Page 30. Capitalize ‘Owner’ in the 1st line of the paragraph immediately preceeding Requirement R3. Insert ‘Requirement’ in front of R5 in the last line of the paragraph immediately preceeding Requirement R6. Spell out TO and TOP throughout the document. RSAW: The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states ‘…any risk assessments conducted prior to the effective date of this standard are not relevant…’ is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there ‘This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.’ We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective. Replace ‘with’ with ‘within’ in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2. Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4. The phrase ‘and compensating mitigating measures’ in the 4th row

in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Group
Colorado Springs Utilities
Shannon Fair
CSU agrees with APPA comments with exception to the confidentiality section, please see CSU's comments below. CONFIDENTIALITY Publicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background: 7. Critical Facilities Information Records and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS: R1.3 All records and information related to the risk assessments conducted of this standard are exempt from public disclosure. R3.2 All records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard are exempt from public disclosure. R4.4 All records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 of this standard are exempt from public disclosure. Adding confidential in the standard would create undo compliance burden and auditing challenges.

Yes
Yes
Yes
Yes
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
No
Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is NRECA's understanding that a "station" equates to a switchyard that does not include transformers; and a "substation" is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
No
R1.1 – NRECA recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straightforward than a 2.5 year focus and it's easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. R2 – The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word "should," not "shall" or "require." The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what "verify" means in the standard. Guidance and rationale is helpful, but does not carry to legal weight of the standard language. R2.1 – This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. Are

there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in the NERC facility ratings alert responses. How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired – this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. R2.2 – This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. R2.4 – The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity R3.1 – The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. NRECA believes 30 days is more appropriate timeframe for this requirement.
No
It's unclear how an auditor will judge compliance with R4 and its subrequirements as it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. R5.1 – NRECA strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement, and resiliency will be next to impossible to audit. 5.3 – After the word "modifications " add ",if any," as this is a possibile outcome. R6 – Same as comments on R2 in Question 2 above. and R2.1. R6.1.1 – NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides for the necessary skills under this standard. R6.1.2 – It is highly unlikely that the ERO is going to approve consultants for industry use. This should be removed. R6.1.3 – All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. R6.1.4 – It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Yes
Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.

Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
Yes
Yes
Yes
ATC supports the draft standard, with the realization that the aggressive time line has raised a broad range of issues or ambiguities resulting from the use of vague language or generic terms. While ATC understands the necessity for this approach, given the compressed timeframe directed by the FERC Order, the project's condensed timeline may not have afforded for the necessary and careful consideration of these terms. Improved guidance around the application of generic terms would increase clarity and help the industry. ATC also supports a follow up effort commensurate with typical standards drafting processes and timeframes to allow for further consideration, improvement, and cleaner language to assure effective implementation of the standard. An example of language like this is in Requirement R1, which includes the vague terminology of "widespread instability, uncontrolled separation, or Cascading." Risk assessment findings can vary significantly depending on the assumptions, criteria, and methodology used for the assessment, and a more thoughtful use of terms could provide for a more uniform risk assessment basis.
Individual
Brian Evans-Mongeon
Utility Services
No
We have seen in the previous versions of the CIP standards that "Risk Assessments" are not performed consistently, and create more problems than they solve, and even violation determinations. The solution in CIP-014 to this inherent problem seems to just add another level of review, but there is no guarantee of consistency within these assessments. Additionally, it seems the drafting team is suggesting a single assessment ("Concurrent with R1 study" specified in R2), this this might eliminate the review stage all together. A clear applicability section with a "brightline" approach would be more appropriate and consistent with the progression of the CIP standards overall. Otherwise, what prevents an auditor from making a determination that the assessment performed was not sufficient or incomplete, even with a 3rd party validation? Entities need a clear definition to avoid the problems of the past. If the drafting team wants to limit the scope of Facilities this could be detailed in the "Exemptions" portion of the "Applicability" section of the standard. 1. The "Exemption"

section needs to be clarified. If this applies to the entire section number it 4.2. If it is only applicable to the last bullet it is under give it the appropriate number (4.1.2.1) Suggested re-write 4. Applicability: 4.1. Functional Entities: 4.1.1 Transmission Owner 4.1.2 Transmission Operator 4.2. Applicable Facilities: The following Facilities, systems, and equipment, owned or operated by each Responsible Entity in 4.1 above are those to which these requirements are applicable. 4.2.1 Transmission Facility operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. 4.2.2 Transmission Facility that operate between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. ADD TABLE HERE 4.2.3 Transmission Facility at a single station or substation location that is identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies. 4.2.4 Transmission Facility at a single station or substation whose unplanned unavailability would result in the loss of at least 3000 MW of generation. 4.2.5 Control Center that controls: 4.2.5.1 Transmission Facilities identified by identification under 4.2.1 through 4.2.4; or 4.2.5.2 Two or more Facilities which contain a Cyber System(s) which have been identified as a High or Medium Impact BES Cyber System. 4.2.6 Exemptions: 4.2.6.1 All facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission. 4.2.6.2 Transmission station or substation connected to only one other Transmission station or substation. 4.2.6.3 Transmission station or substation that does not operate above 200kV. 4.2.6.4 control centers not designated as a “primary control center”
No
1. What is a Transmission “station”? What is the definition of station and what is it intended to cover that substation does not. Generally in the NERC glossary “station” is associated with Generation, not Transmission. 2. There is a concern between R1 and R5. a. R1 states that substations planned to be in service within 24 months should be identified, which would presumably be for stations under construction. b. R5 will then require a Physical Security plan to be in place within 120 days of identification, regardless of the current status of the station. c. Possibly adjust language to allow sites under construction to have the later of 120 days or the operation date of the station. 3. R1.2 should be reworded: “The TO shall identify the primary Control Center with operational authority of each Facility identified in the R1 risk assessment.” 4. R2, if the assessments are concurrent, could this be a joint effort, with the result being 1 report? 5. R2.1, “unaffiliated” needs some clarification. Is this unaffiliated with the TO in any way? Could the TO use their Planning Coordinator, Transmission Planner or RC for the assessment, or do they need to seek out an entity from another region?
Yes

1. R4, what is the time frame for the evaluations? Is this to be conducted during the 30 or 60 month cycle outlined in R2 or more frequently? 2. R6.1, These are all “or” statements and 6.1.1 through 6.1.4 should be bullets, not numbers (this is outlined in the CIP-002-5 page 6, and should maintain consistency with the CIP standards format). 3. R6, Does the ERO have to approve of the third party reviewer? Is there going to be a criteria to determine “demonstrated physical security expertise”?
Yes
1 “primary control center” is confusing. NERC has a defined term “Control Center” which is intentionally not being used. What is the intent of not using the defined term? If the undefined term remains in use more clarity needs to be given on “primary control center”. 2. what is the definition of “widespread?” Does this mean outside of a Balancing Authority Area, outside of a Region or outside of an interconnection? More clarity is needed in the term. Additionally, TO’s may not have the data required to perform this type of assessment. There needs to be process in place for the TOs to obtain the data required to perform the appropriate assessment. 3. The SDT should review projects such as PRC-006 or MOD C, and define groups within the requirements to reduce the length of requirements. For example R4 could be reduced to the following, making the requirement easier to read and adding much needed clarity: “Each Applicable Entity shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Applicable Facilities as identified in R1 and verified in R2. The evaluation shall consider the following:… “ RSAW Comment: R1 “Evidence Requested” section doesn’t provide a time frame for the first assessment, no assessment prior to effective date will be considered, but there must be an assessment completed before the effective date to be complaint. This is a catch 22.
Individual
Dan Inman
Minnkota Power Cooperative
Yes
Yes
Yes
Yes
In the “Draft_RSAW_CIP-014-1_v1_2014_0409.pdf” document, on page 4 of 22, there is a Note to Auditors Concerning Third Party Verifications and Reviews. In this section there is a mention to the “concept of reliance means using the work of others to avoid duplication of efforts”. While the reference to “duplication” was in regards to unaffiliated third party verifications and reviews, we appreciate the SDT be congnitive of “duplication of efforts” as their developing the Standard and the RSAW. With the very restrictive timeframe for which the development of the Standard was required, this concept can get lost. We did see another

area in the Standard CIP-014-1 R5.2, which may be considered “duplication of efforts”. CIP-014-1 R5.2 states, the TO/TOP should have in their physical security plan(s) law enforcement contact and coordination information. On June 20, 2013, FERC approved Reliability Standard EOP-004-2, which identified types of reportable events and thresholds for reporting, requires responsible entities to have an operating plan for reporting applicable events to NERC and other entities (including law enforcement), and requires reporting of threshold events with a 24 hour period (Docket No. RD13-3-000). This Standard covers the need to incorporate law enforcement contacts in the operating plan. Requesting this type of information in both the operating plan required in EOP-004-2 and physical security plan in CIP-014-1 is a “duplication of efforts”. MPC believes the intent for CIP-014-1 was to identify and mitigate physical security risks, while the intent for EOP-004-2 is to improve reliability of the BES by requiring the reporting of events by Responsible Entities. MPC suggests removing Requirement 5.2 in CIP-014-1.
Individual
John Allen
City Utilities of Springfield, Missouri
Agree
APPA
Individual
kim moulton
Vermont Transco LLC
Yes
While we do agree with the need for the standard and the importance of it we do have comments on the proposed standard. The intention of this standard is to protect those facilities that are most critical to the bulk electric system. The CIP-002-5.1 criteria brings into play many facilities that while deemed critical to an entity are not likely critical to this standards definition and would not cause wide area impact.
Yes
Specifically the filtering of assets. While starting with CIP-002-5.1 as a starting point, the amount of analysis and assessment to determine if these facilities are critical and applicable to this standard may not be possible in the timeline proposed for this standard if a full transmission planning analysis will be needed. Many planning analysis performed previously by entities were not assessed to the specific defininition included in this requirement and therefore could require considerable work to be performed to analyze. The wording suggests that a full transmission planning assessment should be performed for all CIP-002-5.1 facilities and not to just those an entity feels may cause wide area impact. What if you do not agree with the third parties review of your assessment? what evidence will be required to prove that you do not need to agree with their assessment? If an entity identifies a facility as critical does this require that the control center operating this facility must also have a full physical security plan per the requirements later in the standard?

Yes
how long will and entity have to complete their plans designed due to the evaluation of threats? It appears that the standard is saying that you must develop a plan and a timeline to complete your actions associated with the plan. What if a timeline needs to be adjusted at some point, will an entity have to notify their RRO? Or just track all changes and their need to provide to an auditor during a full audit of the standard?
No
Group
Western Area Power Administration
Lloyd A. Linke
Yes
Western agrees with what we understand as the applicability, based on the CIP-014 Workshops. However, we have some concern with the undefined term 'collector bus facility'. Without a definition for collector bus facility we are concerned that some parties may consider the entire switchyard at a generating station as a collector bus facility. Based on the discussion during the CIP-014 Workshops we do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
Yes
Western agrees with the approach of using Requirements R1 and R2 to identify whether an entity is subject to Requirements R4-R6. However, we suggest that the drafting team modify the term "risk assessment" to "BES impact assessment." In the physical security community, the term "risk assessment" generally refers to "The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel." See ASIS International, General Security Risk Assessment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term "BES impact assessment" so it is clear that the initial evaluation is of risk to the BES if the substation is damaged or rendered inoperable. Western recommends revising R1 1.1 to: "Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment." This would consolidate the two bulleted actions and make them equally applicable. We believe a 60 month interval would be a more appropriate period for this type of assessment. Western suggest the drafting team clarify requirement 2.1, which directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment; however, these NERC functional entity designations do not appear in the applicability section of the standard. We also suggest reconsidering the short 90-day period to ensure verification of the risk assessment. This may not allow every Transmission Owner to establish a contract with an unaffiliated verifying entity during the standard's implementation time period.

Yes
: We recommend striking the qualifier regarding the ASIS “Certified Protection Professional or Physical Security Professional” from the standard R6-6.1.1 as it is inclusive of only one organization and may not provide the best support for each entity . Simply having these certifications does not guarantee the necessary knowledge to perform this unique work. We believe the language does not support the intent of the FERC Order as identified in paragraph 11. We request the Drafting Team clarify the scope of the third party review process identified in R6 and tie the requirement to a specific and established method as consistent in accepted practices, such as the ISO processes. We recommend the third party review process be clarified as a review of the primary entity’s adherence to their established processes in evaluating threats and vulnerably, as well as their security plan(s). We believe the current audits conducted by the regional entities satisfy the third party review process as identified in the FERC Order, paragraph 11. We do not believe R6-6.4 adequately protects the sensitive information contained in the risk, threat, and vulnerability assessments, or the security plan(s). These reports may contain sensitive and/or classified information, or otherwise information that if released would jeopardize the BES, with little to no penalty for an offending party.
Yes
In the VSL for requirement R5, in all four severity levels, states that the security plans need to be developed for the facilities “identified in requirement R1”. However Requirement R5 only requires the plans to be developed for facilities ‘identified in Requirement R1 and verified according to Requirement R2,”. The VSL should be modified to include the statement ‘and verified according to Requirement R2. The first row in the Table, in the RSAW, describing the evidence required in requirement R1, it states that any risk assessments conducted prior to the effective date of this standard are not relevant. The Implementation Plan states that “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” There appears to be a conflict between these two statements, unless the intent is that the initial risk assessment needs to be completed on the effective date. Also, normally, unless the implementation plan provides a different time line, you need to be compliant by the effective date. In the RSAW for requirement R6 the fourth row in the Evidence Requested table, it asks for evidence that includes the “reasons or compensating mitigating measures for not implementing the recommendations for the reviewing party.” Requirement R6.3 of the standard only requires the Transmission Owner or Transmission Operator to “Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.” These two statements should be clarified in order to ensure consistent enforcement.
Individual
Lynnae Wilson
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.
Yes

Vectren supports the use of the CIP-002-5.1 medium impact criteria. This approach focuses on the facilities that could have a true adverse impact to the Bulk Electric System and provides consistency with approved standards.

No

Specifically, Vectren recommends that R2 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to designate registered Planning Coordinators, Transmission Planners, or Reliability Coordinators as the approved verifiers for entity risk assessments AND to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later – leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

No

Specifically, Vectren recommends that R6 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later – leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

Yes

Vectren recognizes that this drafting effort required significant contraction of drafting and approval processes, and Vectren appreciates the work of the drafting team. Vectren is

supportive of the goals of the standard, supports R1, R3, R4 and R5. Vectren urges the drafting team, NERC and FERC to remove entirely or add detail to the requirements R2 and R6, and to add specific audit criteria in the RSAWs, so that entities can have some confidence that their risk assessments performed in good faith, will be considered compliant with this Standard.
Individual
Venona Greaff
Occidental Chemical Corporation
Agree
Ingleside Cogeneration, LP
Group
Texas RE
Derrick Davis
Yes
The applicability should include the TP, PC, RC, and the unaffiliated entity as they are noted in this standard.
No
1. For R1, the Transmission Owner is not the appropriate entity to conduct the type of transmission analysis that the requirement describes. It seems like a more logical process would be for the Transmission Planner to conduct an analysis of all substations meeting the applicability in 4.1.1.1 thru 4.1.1.4, and then, if the removal of a substation results in Cascading, instability, or uncontrolled separation, the TP will then notify the TO & TOP to conduct the security threat evaluation per R4 at only those substations identified by the TP. 2. R1 - A “risk assessment” pertains to the physical security of Transmission Facilities while a “risk-based assessment” pertains to identification of Critical Assets and Critical Cyber Assets. The two phrases are too similar in meaning to each other, but possess differing meanings and intents. 3. For R2, if the approach described in #1 is accepted, it may also satisfy R2 in those cases where the TP is independent from the TO. The independent verification would also be the responsibility of the TP, utilizing another TP, the PC, the RC, or an unaffiliated entity as described in the current language. 4. For R3, if the approach described in #1 is accepted, the initial notification to the TOP would originate from the TP.
No
1. The sequence and timelines for R5 and R6 need to be reviewed. R5 states the TO “shall develop and implement” the security plan within 120 calendar days of completion of R2. R6 states the 3rd party evaluation can occur concurrently with or after completion of R5. It seems like the 3rd party evaluation should be completed before the plan is implemented in R5, otherwise the entity may be planning for or implementing measures that may not be appropriate for the risk level. 2. R6 also 3. Also, who evaluates the implementation phase of security plan and whether or not it was implemented correctly or if the plan was effective? There should be an entity assigned for this task. There should be an exercise (like GridEx) to

test the plan. 4. The third party reviewer could be the same entity in R2 and R6. This could be a question of independence. It also does not indicate the third party actually verifies the implementation of the security plan(s) in R6. This does not permit the Compliance Enforcement Agency to place reliance upon the work of the third party.
Yes
Several places in the standard refer to notifying the Transmission Operator for stations that meet the higher risk profiles. However, the language is not clear as to what is expected from the Transmission Operators when a physical security incident occurs at one of those substations during real-time operations. Finally, this entire process can exceed four hundred days, which is excessive.
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
No
FMPA commends the efforts of the SDT to lay out an excellent process for risk assessment in accordance with the FERC Order in such a short time frame. We only have few comments. WHAT DOES “CONTROL CENTER” MEAN Is there a signifance for not using the capitalized term of Control Center throughout the standard? It seems to FMPA that the defined term “Control Center” ought to be used. If the intent is that “control center” and “Control Center” mean two different things, then, what does “control center” mean? If the intent is to include large TOs that may be part of a large TOP, such as a large utility in an RTO, that do not have Control Centers; then, FMPA recommends using a different term such as “the location of the SCADA system that has remote control of breakers associated with the identified substation/station” or similar might avoid confusion. WHAT DOES “UNAFFILIATED” MEAN The term “unaffiliated” may be a source of ambiguity and conflict without further definition. For instance, dictionary.com defines affiliated as: “being in close formal or informal association; related” So, this would imply that peer members of the Transmission Forum are affiliated, which we do not believe is the intent of the SDT. FMAP believes the SDT’s intent is as Black’s Law Dictionary defines affiliate: “1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.”; which would mean that peers within the Transmission Forum are unaffiliated, but subsidiaries of a company are affiliated, or members of a Joint Action Agency are affiliated. It also aligns with FERC’s definitions for Affiliate in their market based rates regulations 18 C.F.R. 35.36(a)(9) and in the Pro Forma OATT. FMPA suggests using a footnote to clarify use of the term unaffiliated, such as “Use of the term unaffiliated is in relation to Black’s Law Disctionary defition for affiliated: ‘1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.’”

PROPER QUALIFICATIONS FOR RISK ASSESSMENT VERIFICATION FMPA appreciates the challenges of defining qualification for independent verifiers while offering registered entities a broad choice for selection. We interpret that requirements R2 and R6 grant the applicable entity sole authority to choose the 3rd party verifier as long as they meet the qualifications contained within those requirements. Is FMPA correct in that interpretation? CHANGE MANAGEMENT OF THE RISK ASSESSMENT The standard is somewhat ambiguous on what happens if the responsible entity chooses to revise it's risk assessment of R1 sooner than the required 30 or 60 calendar months. Does every minor revision to the risk assessment require another 3rd party review? Or would only major system changes (e.g., due to adding a major new investment in the power system like a new 500 kV line) require review? Or regardless of system changes, would the review occur once every 30/60 months? FMPA suggests clarification to R2 to say that minor revisions to the risk assessment due to minor power system changes in between the 30/60 month periods do not need a separate 3rd party verification.

No

Again, FMPA commends the SDT for a job well done. Just a few minor comments. See response to question 1 concerning use of the terms "control center" and "unaffiliated". CHANGE MANAGEMENT OF THE VULNERABILITY ASSESSMENT AND SECURITY PLAN Similar to our comments regarding change management of the risk assessment, it is ambiguous as to how we would implement change management related to the vulnerability assessment and security plans. R4 has no periodicity requirement, but, instead seems to require responsible entities to continuously reevaluate their vulnerability assessments in response to events listed in bullets 4.1, 4.2 and 4.3. If the entity changes their vulnerability assessment to include new threats, does every revision require a new 3rd party review? How do we come to agreement what constitutes a valid "trigger" for a new vulnerability assessment? It seems to imply that each of us would need to have an independent 3rd party on retainer to review our assessment of every intelligence or threat warning from governmental or regulatory agencies, or new attacks that each entity becomes aware of. Is that the intent? If so, what consititues a "warning", e.g., is it an "official" warning through some sort of official channel, such as a NERC Alert? If so, what happens if an entity decided to act on an "unofficial warning", such as a media release, to revise their vulnerability assessment – would that also need a 3rd party review? FMPA suggest clarifying 4.3 with "Official intelligence or threat warnings …". R5 seems overly ambitious. 120 days, or 4 months, is not a lot of time to perform a vulnerability assessment and develop and implement a security plan, especially in response to a newly identified threat vector/warning, and especially considering that a revised security plan may include capital investments in measures like new enclosures, vehice barriers, or the like. Is the intent that a security plan could be a phased approach, e.g., implement an interim security plan within 120 days while future improvements to that plan take longer? If so, then the language of the requirement ought to reflect that intent. FMPA suggest a modification to R5 such as: "… shall develop and implement the first phase of a documented physical security plan(s) … within 120 calendar days …" In addition, R5 does not seem to fit temporally with R2 and R4 well. R2 requires periodic risk assessments every 30/60 months. R4 seems to require changes to vulnerability assessments in response to newly known threat vectors. The timing

of R5 refers to R2: "… within 120 calendar days following the completionof R2" with no reference to a revision to the vulnerability assessment. This causes FMPA to belevie that revisions to the security plan as a result of a new threat vector and a revised vulnerability assessment of R4 would not need to be required until 120 days following the next periodic risk assessment of R2. Is that the intent? If that is the intent, if an entity chooses to revise the security plan earlier, would that then need an 3rd party verification at that time, or at the time of the periodic risk assessment?
Yes
FMPA has concerns for the RSAW and the lack of direction to auditors from the RSAW concerning the scope of their review. The auditor should not have a subjective decision regarding the sufficiency of the risk assessment, vulnerability assessment or security plan of the TO/TOP. The unaffiliated 3rd party is the source of qualified expert subjective opinion on the sufficiency of the risk assessment, vulnerability assessment and security plan. As such, the RSAW ought to clearly define the scope of the auditor's review of the risk assessment, vulnerability assessment and security plan. FMPA suggests rewording the "Compliance Assessment Approach"portions of the RSAW that call for these reviews to read something like the following (specific to R1): Review the entity's risk assessment to answer the following: a. Were all of the entity's assets, existing and planned to be in service within 24 months of the date of the documented risk assessment, and applicable to the standard (Applicability Section 4.1.1), included in the assessment? b. Was a transmission analysis or transmission analyses identified and documented to evaluate whether any applicable Transmission station(s) and Transmission substation(s), if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? The auditor is not to evaluate the sufficiency of such analyses; but rather whether such analysis was documented. c. Was the assessment conducted within the timeframes identified in bullet 1.1? d. Was the primary control center(s) identified in accordance with bullet 1.2?
Individual
Thomas Foltz
American Electric Power
Yes
Yes
Yes
Yes
It is AEP's understanding that regarding R5, the phrase "develop and implement a documented physical security plan…within 120 calendar days" means that, within 120 days, the physical security plan must be completed and that the entity is working toward implementing the plan and does not mean that the plan must be fully implemented within

120 days. AEP urges the clarification of that expectation within R5 so that the requirement is unambiguous. Regarding R6.4, please clarify whether the procedures for protecting sensitive or confidential information would include suitable terms and conditions within a third party contract.
Group
Duke Energy
Michael Lowman
Yes
Yes
Yes
Yes
(1) Duke Energy suggests that language should be incorporated either in the proposed standard or RSAW to allow for the flexibility in modifying the timeline specified in R5.3. We believe there are unforeseen circumstances that could occur which would result in the proposed timeline shifting from the intended completion date. Examples include, but are not limited to: a. Unplanned outage of transmission or generation facilities that results in canceling scheduled work. b. BES reliability concerns should the facility be out of service for a short or extended period of time. c. Third party vendor's availability in implementing recommendations made by an entity or unaffiliated third party verifier. For these reasons, we believe a provision is needed to allow for this type of flexibility in modifying the timeline specified in R5.3.
Individual
Anthony Jablonski
ReliabilityFirst
Yes
ReliabilityFirst supplies the following comments for consideration: 1. ReliabilityFirst believes there may be a perceived disconnect between the Applicability Section and Requirements 5 and 6. Requirements 5 and 6 introduce new requirements surrounding the Transmission Owners "primary control center" though the "primary control center" is not listed within the Applicability section as an asset the Transmission Owner owns that is included in the standard. Consideration may be given to adding "primary control center" under section 4.1.1. [Note: Since "Control Center" is a NERC defined term, this term should be capitalized throughout the standard.] 2. Applicability section 4.1.1.4 - ReliabilityFirst believes the term "as essential" is ambiguous and may cause unintended compliance monitoring implications. ReliabilityFirst recommends the following for consideration: "Transmission Facilities identified

[in] Nuclear Plant Interface Requirements [which provide offsite power].” ReliabilityFirst believes the recommended language addresses the intent of the SDT.
Yes
ReliabilityFirst supplies the following comments for consideration: 1.Requirement R1 - ReliabilityFirst believes there may be a gap in the timing of performing the risk assessment for new Transmission stations and Transmission substations which are planned outside the 24 month window as required in Requirement R1. For example, as written, if a new Transmission stations or Transmission substation is planned for month 25, it would not be included within the initial risk assessment. Thus, there is a potential for this new Transmission stations or Transmission substation to not be assessed for 30 calendar months (for a Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable …) or 60 calendar months (for a Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability…” With the potential gap in assessing new Transmission stations and Transmission substations being so long, ReliabilityFirst believes reliability may be compromised. For these reasons, ReliabilityFirst recommends the following for consideration: “Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months)…” and including a new bullet under Part 1.1 which states “At least prior to the implementation of all new Transmission stations and Transmission substations (if not assessed within the initial or subsequent risk assessment)” 2. Requirement R3 part 3.1 - From a standards writing perspective, if there is only one sub-part, ReliabilityFirst recommends including it within the Parent requirement R3. Typically sub-parts are only included if there are more than one.
Yes
ReliabilityFirst supplies the following comments for consideration: 1. Requirement R5 - ReliabilityFirst requests clarification on why the term “primary control center” is used throughout the document instead of just “control center”, as it seems both a primary and secondary control center would be of equal importance (and have similar vulnerabilities) to reliability.
Individual
Larry Watt
Lakeland Electric
Agree
Florida Municipal Power Agency (FMPA)
Individual
Donald E Nelson
MA Dept. of Public Utilities
Agree

Agree with the comments made by NPCC.
Individual
Andrew Gallo
City of Austin dba Austin Energy
Agree
American Public Power Association (APPA). In addition, Austin Energy states the following: The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this Standard may be subject to disclosure under state open records laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard designating the produced, gathered, used and maintained records related to compliance with this Standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure.
Individual
Kevin Lyons
Central Iowa Power Cooperative
Agree
ACES
Group
Peak Reliability
Jared Shakespeare
Yes
Yes
Peak believes the RC entity should perform the R2 verification because the RC has the wide-area view in the Western Interconnection. The alternative would be to have individual transmission entities perform varied verifications, which could result in inconsistent methodologies and results.
No
Individual
Robert Trowbridge
Consumers Energy Company

Yes
With Michigan situated as a peninsula, Michigan infrastructure may be at a lesser risk, based on the limited number of interconnect avenues into and out of our system. Meaning the highest level of criticality likely would be identified as those key interconnect points, and not the entirety of our system. From our experience with the blackout of August 2003, BES implications were centered in southeast Michigan and although affected, we were able to successfully minimize/sustain our base load generation requirements. Any substation targeted in Michigan may not have a cascading effect on the BES.
No
We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
No
We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
Yes
Develop a requirement to protect information shared between entities and third party organizations. Requirement number 6 should be revised to state “…third party reviewer that is either…” 6.1.1 or 6.1.2 or 6.1.3 or 6.1.4. R6 seems vague and should be revised
Individual
Chantal Mazza
Hydro Québec TransÉnergie
Yes
No
Hydro-Quebec TransEnergie (HQT) agrees with this approach but requests that the SDT remove the term "unaffiliated" from Requirements R2 and R6.1 HQT notes that the term "unaffiliated" is not used in FERC Order 146. Paragraph 11 of the Order states "In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator." Moreover, it appears that it is not FERC's intent to introduce this restriction regarding the choice of a third party. HQT therefore believes that the use of the term “unaffiliated” goes above and beyond what was stipulated in the FERC Order. Furthermore, the term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities (RC, PC and TP) that the SDT is seeking in the draft standard. The Reliability Model uses the term "functional entity" to apply to a class of entities without making reference to specific organizations that register as functional entities. For some Canadian jurisdictions, the use of the term "unaffiliated" renders the standard more stringent due to the fact that certain Canadian entities such as Hydro-Québec TransÉnergie are simultaneously

registered as TO, TOP, PC and RC. For integrated modeled entities, the restriction of available options that would otherwise be available (such as selecting a PC, TP or RC for the risk assessment verification under R2), makes it difficult to identify an entity with the required expertise capable of performing the reviews stipulated in the standard. HQT believes that the risk assessment of a TO should only be verified by the RC or the PC that has supervision (real-time or planning) over the said TO's assets because only the RC or the PC can ensure a comprehensive approach to critical facility identification that considers the reliability of an entire area. For these reasons, HQT believes that the expression "third party" alone is sufficient and consistent with the expressed concerns in the FERC Order.
No
The same comments regarding the term "unaffiliated" in Question 2 above apply to R6. HQT believes that the SDT should remain general about the security measures that should be put in place. Requirement R5.1 states "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." We believe that rather than the standard dictate what type of measures are to be implemented, it should be rephrased to remain general and use similar language that is used in paragraph 9 of the FERC order. Suggest rewording the requirement to "Resiliency or security measures designed to protect against potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.".
Yes
The following are suggestions to facilitate reading of the standard, as well as its future translation: All requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary. R1: Remove "transmission analysis" from the sentence "The initial and subsequent risk assessments shall consist of transmission analysis or transmission analyses designed to …" We believe this repetition is unnecessary. R2.2: The first part applies to an entity that is not subject to the standard and should be removed from the standard. R2.3: Replace the word "identification" with "assessment". Remove the word "either" Rephrase R4, R5 and R6 (add "a"): " ...a transmission substation, or a primary control center". R4 and R5: Remove the part "…that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation". It only complicates the reading of the requirement (the TOP is not notified by the TO unless it has operational control over an asset identified in R1). If the first parts of R4, R5 and R6 are intended to identify the functional entities to which the requirement applies, we suggest "… and each Transmission Operator notified by a Transmission Owner under requirement R3, shall …" for the TOP portion (line 3 to 6 of R4, R5 and R6). We believe that it would greatly improve clarity and readability of the requirements. R6.1: rephrase to "from one of the following". Furthermore, the numbers 6.1.1 to 6.1.4 should be replaced with bullets as is the case in R1.1, R2.1, and R2.2. Rephrase R6.1 and R6.1.1 to reflect the language used in the rationale. We believe limiting the reviewer to someone with a CPP or PSP certification goes beyond what the FERC order requesting. Suggest rephrasing to "with appropriate expertise of the evaluation performed". Guidelines and Technical Basis on requirement R1: HQT agrees with the fact that the TO has discretion to

choose the specific method to establish the risk assessment, and that it is relevant that the Guidelines proposes examples. However, the proposed example of "removing all lines to a single Transmission station" seems to present a very stringent impact considering a physical attack on a facility. We ask the SDT to propose others less stringent examples that would be more in line with realistic physical attack, such as loss of a large section according to physical organisation of the facility, or loss of all main transformers, etc.
Group
Dominion
Connie Lowe
Yes
No
Measure M1 - R1.2 -- Measure M1 does not address sub-requirement R1.2 which requires the Transmission Owner to identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment. Dominion recommends the SDT determine whether M1 should include the control center. R2.3 - Relative to R2.3, Dominion does not agree that the TO should have to document the technical basis for retaining assets that have been suggested for removal by the third party. R3 - Dominion suggests R3 be revised to strike the words ‘and verified according to Requirement R2’, and changing R2 to R1.2 in the next two instances where R2 is mentioned. This is due to the reason there is nothing included in R2 that requires verifing primary control centers.
No
R5 and R6 are written for the initial risk assessment and don’t necessarily apply for subsequent risk assessments. Is the expectation that 3rd party reviews be performed for R4 and R5 every time R1/R2 is run, particularly if there are no changes? Dominion recommends that the SDT modify this in the event the R1 list changes (ie: add stations) to require a subsequent R4/R5 reassessment. If stations drop off, or no change to R1 list for subsequent assessments, then subsequent R4/R5 reassessment is not required. R6 - Through continuous improvement processes and lessons learned, there will be expected changes to the security plan(s). What changes are allowed to the security plan(s) without triggering a 3rd party review?
No
Individual
Michiko Sell
Public Utility District No. 2 of Grant County, WA
Public Utility District No. 2 of Grant County, WA
Yes

Language contained in R1 does not align the performance of risk assessments of Transmission stations and Transmission substations with the actual commissioning or energization of such facilities. To ensure that risk assessments and subsequent risk assessments address existing and planned Transmission stations and Transmission substations to be in service within a risk assessment window the following edits are recommended to R1: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months) .. 1.1. Subsequent risk assessments shall be performed at least once every 30 calendar months. (this would apply to all applicable TOs) GCPD also supports comments made by APPA regarding the insertion of the language addressing Confidentiality and treatment of Critical Facilities Information. GCPD's suggested language is as follows: Risk assessments and evaluations of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure.
Yes
R2 references primary control center(s). Since Control Center is a NERC defined term GCPD suggests that all references to the Control Center be capitalized within the Standard and that "primary" be defined within the standard to not include "back-up" Control Center(s).
Yes
GCPD appreciates the flexibility built into the Standard language that allows tailored evaluations of potential threats and vulnerabilities to its own facilities. GCPD supports APPA's suggested edits to the Standard to enhance clarity of requirements under R4, R4.1 & R4.2. In addition, APPA's suggested removal of "and implement" under R5 clarifies that the intent of R5 is to develop the physical security plan, not fully implement the plan within 120 calendar days. This would better align the Standard language contained in R5.3.
Yes
GCPD feels that the implementation schedule is somewhat arbitrary and demonstating compliance with the implementation schedule conflicts with language contained in the proposed RSAW. GCPD supports RSAW edits as proposed by APPA to address these discrepancies. GCPD proposes the following edits to Requirement language addressing implementation timing to allow for enforceable and auditable time lines not dependent upon the unique completion date of the initial risk assessments conducted by the RE. 2.2. ...The Transmission Owner shall ensure the verification of the initial risk assessment performed under Requirement R1 is completed within 90 calendar days following the effective date of this Standard. Subsequent risk assessments shall have verifications completed within 90 calendars days of completion of the risk assessment. R5. ...and primary Control Center(s) within 210 calendar days following the effective date of this Standard. Changes to recognized applicable facilities under this Standard as identified under Requirement R1 and verified according to Requirement R2, shall require review of the physical security plan(s) within 90

calendar days of completion of associated risk assessments. ... General commentary: in October 2012 the Cost Effective Analysis Process (CEAP) was approved for a “pilot”. The NERC CEAP was intended to integrate cost consideration and effectiveness into the development of new and revised standards. The first phase of the CEAP was to be implemented during the SAR stage to determine cost impact and identify “order of magnitude” or potentially egregious costs, to determine if a proposed standard will meet or exceed an adequate level of reliability, and what potential risks are being mitigated. The second phase was to be conducted later in the standard development process and afford the industry the opportunity to offer more cost efficient solutions that may be equally effective to achieving the reliability intent of the draft standard. This report would be posted at the time the standard is balloted. The report was intended to present the data collected in a manner which will provide the industry with representative cost implementation and effectiveness information to allow a more informed choice during balloting. Based upon the urgent nature of this Standard, phase two would need to be applied. The CIP-014 Standard requires costs to be incurred to comply with Requirement R5. In addition, there may be substantial costs incurred to implement the Physicial Security Plan(s). The CIP-014 Standard is an ideal standard upon which to exercise the CEAP. The information resulting from the CEAP would be beneficial not only to government officials, but also the industry as a whole.
Individual
Brett Holland
Kansas City Power & Light
No
There is a use of the term "critical" being used in several NERC Standards, which can cause unintended confusion. Since the applicability of this draft Standard is derived from the approved CIP-002-5.1, can this proposed Standard be added as a revision to CIP-002-5.1?
No
In R1, we have concerns about the ambiguity associated with the term "assessments". Can you provide examples of the types of assessments that would be acceptable to meet R1 and that would be CIP audit worthy in the future. We have the same concern in R2 with the term "third-party". Will there be a list of pre-approved third party contractors or will the RE's review and approve a third-party at the request of the registered entity prior to their use in the verification process as described in R2?
No
Same comments about "third-party" from Question 2.
No
Group
APPA
Joe Tarantino
American Public Power Association (APPA)

SMUD supports the APPA comments and is specifically concerned that records and information developed and maintained under each of the requirements for this standard are afforded the necessary protection through an introduced section, #7 Critical Facilities Information. We respectfully ask the Standard Drafting Team to ensure that AUTHORIZED ACCESS to information pertains to ANY RECORD AND INFORMATION associated with the Physical Security Standard.
Individual
Nick Braden
Modesto Irrigation District
Modesto Irrigation District supports the comments submitted by American Public Power Association/Large Public Power Council
No
MID agrees that maintaining selection criteria consistent with CIP-002-5 is a prudent approach. However, if a facility is worthy of protection against a cyber attack, why is that same facility not worthy of consideration and evaluation for a potential physical attack? Inclusion of 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' as an additional criteria is also prudent. These criteria focus on the immediate impact of the physical attack. What is missing is the longer term impact - if serious physical damage is the result, can the damaged system perform adequately during subsequent peak loading periods? MID understands that these changes would extent the scope of the standards coverage beyond what was included in the FERC order. MID would like to respectfully suggest that the FERC order is a step in the right direction but did not fully consider all of the potential physical attacks that could cause 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' or impair long term reliability of the system. MID feels that in responding to the FERC order, it would be acceptable to ‘do the right thing’ and step up to the challenge and evaluate all facilities identified in CIP-002-5 as high or medium impact the system against possible physical attacks.
Yes
Yes
No
Individual
Dixie Wells
Lower Colorado River Authority
Agree

Lower Colorado River Authority
Individual
Alan Johnson
NRG Energy, Inc.
Yes
This standard should not address generation interconnection facilities because the BES is designed to withstand the loss of generation facilities through the use of regional reserves.
Yes
NRG agrees the approach described in Requirements 1 through 3 address the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: • Primary control centers are referenced in the “purpose” of the standard, but are not included in the “applicability” section. For clarity, NRG suggests the addition of section 4.1.1.5, stating “Control Centers and backup Control Centers associated with the Transmission stations and Transmission substations identified in requirements 4.1.1.1 through 4.1.1.4.” • R1 directs that the Transmission Owner to perform an initial risk assessment with subsequent studies and include an unaffiliated third party to verify the risk assessment performed. NRG is concerned the standard does not indicate how information shared under this Requirement will be protected and held in confidence. NRG believes the information subject to this standard should be treated as Critical Energy Infrastructure Information (CEII). • R1 is vague in providing guidance as to the criteria to be used in developing the risk assessment. NRG appreciates this is intentional to allow flexibility in developing the assessment. However, this results in the potential for a determination of non-compliance during the audit process. NRG suggests reliance on the CIP-002 standard used for defining Critical Assets, which is based on solid metrics. • R2 seems to allow the same third party to perform both the initial risk assessment and the review of the initial risk assessment, potentially negating the need for a separate review. • R2.2 calls for review of the results of the initial risk assessment by an unaffiliated third party. The standard provides no guidance regarding the criteria (assumptions, contingencies, etc.) to be used for this review, which could provide results differing from the initial assessment. More objective measures should be incorporated.
Yes
NRG agrees the approach described in Requirements 4 through 6 addresses the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: • R5.1 provides no guidelines or examples of how to combat certain threats, or even what threat thresholds require accounting for. NRG appreciates the flexibility built into the requirement. However, NRG is concerned this flexibility could result in “interpretation” issues during future audits of compliance with the standard. • The ability to meet the time horizon commitment for providing the third party assessment of the vulnerabilities and security plan are contingent upon the availability of certified parties that

can adequately perform these assessments. NRG is concerned there may be a lack of qualified resources available to the industry to complete the necessary reviews within the required time frame. • Because the reliability of the bulk power system depends on numerous susbstations all across the nation, it would be more effective to increase the monitoring of the grid to ensure timely, effective re-routing of power when a disruption occurs. • Minimum physical standards should be established within the security plan that include industrial standard chain link fencing with barbed wire topguards; gates secured with chains and locks (not the alloy metal collar around a post); signage that clearly states No Trespassing every 100 ft., or on each perimeter side at small footprints; cameras that are monitored by the appropriate transmission control center, security control center or a contract central monitoring service and capable night viewing to be able to identify intruders.
No
Individual
Curtis Klashinsky
FortisBC
Yes
No
The audit provides an independent review of an entity's application of the standard and therefore, an additional third party review should not be required as described in R2. It is agreed that if a null set is identifed, the rest of the standard does not apply.
No
The third party review of the security plan does not guarantee an objective evaluation as they would be funded by the requesting entity. The standard could state that the entity should follow an industry standard technical guideline. The audit provides an independent review of an entity's application of the industry standard technical guideline and therefore, an additional third party review should not be required as described in R6.
No
Group
New Brunswick Power Corporation
Alan MacNaughton
No
New Brusnwick Power (NB Power) agrees with the “applicability section” but not with portions of the preamble above, in question 1, which expands beyond applicability and states that “Furthermore, the standard drafting team expects many who are “applicable” to the standard will not identify facilities through their Requirement R1 risk assessment and

Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection." To our knowledge there is no evidence to support the standards drafting teams statement that they expect that many of the applicable entities will not identify facilities through R1 and R2. FERC's statement that "we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System" is not sufficient evidence. NB Power is concerned that the cost impact of this standard may be underestimated as a result of this view that the number of critical facilities will be small. Please see comments below with respect to R1 and R2.

No

In general, a TO may not have the capability to conduct a risk assessment to determine if an identified facility that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Such an assessment requires a wide area view of the Interconnection. It is proposed that the risk assessment be conducted by a PC, or RC for the area in which the facility is located. Doing so would satisfy the third party verification requirement as the TO would not be conducting the analysis. It is the opinion of NB Power that the technical details concerning the transmission analysis, in the proposed standard, are overly vague. This could lead to an inconsistent application of the analysis between entities as well as create obstacles with consensus concerning the proposed 3rd party verification. NB Power suggests a clear analysis methodology be drafted to establish a common basis for study criteria with the ability for each entity to apply additional specific requirements for their respective area. For corporate bodies, such as a vertically integrated utilities, that are registered as the RC, TOP, PC, TP and TO for a particular area, it is the opinion of NB Power that the requirement for unaffiliated 3rd party verification is overly stringent and of little value. The verifying party is limited to entities that have transmission planning or analyses experience, or, are registered as a PC, TP, or, RC from an adjacent area. NB Power is of the view that there are no unaffiliated entities with sufficient knowledge of the local transmission system to provide a meaningful verification within a 90 day period. As a government owned utility, NB Power is required to follow procurement processes which will make it difficult to meet the 90 day period for the third party verification. NB Power is also concerned that it could be non-compliant with the requirement if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance. It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated verifying 3rd party in requirement R2.3. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated verifying 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd parties recommendations.

No

NB Power is concerned with the 120 day timeline to implement a physical security plan that would meet the third party verification requirements. Having limited knowledge of physical security issues NB Power will likely rely on the third party verifier to work with NB Power in developing a security plan. NB Power is not aware of any analysis that was done to ensure that there is enough capacity within the “physical security industry” to support the work load increase resulting from the approval of this standard and as such is concerned that 120 days may be insufficient. NB Power is concerned that it could be non-compliant with R6.2 if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance. It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated reviewing 3rd party in requirement. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated reviewing 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to a consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd party’s recommendations.
No
Individual
Mark Wilson
Independent Electricity System Operator
Yes
We agree with the inclusion of the Transmission Owners and Transmission Operators as they have the obligations to conduct an evaluation of the potential threats and vulnerabilities to a physical attack on each of their respective transmission stations/control centres.
No
While the proposed R1 to R3 collectively meet the FERC requirements for having an entity to identify the critical facilities and having the assessments of such identification verified, we believe it is more appropriate that the 3rd party verification be performed by NERC registered entities only (which could be the Reliability Coordinator, Planning Coordinator or Transmission Planner). An entity that has transmission planning or analysis experience may only have an outside equivalent representation of the BES and their ability to conduct an analysis with a “wide area” view of consequences may not be possible. As such, we suggest to revise Requirement 2.1 by eliminating the second bullet point : “An entity that has transmission planning or analysis experience”.
Yes
Individual

Kenn Backholm
Public Utility District No.1 of Snohomish County
Agree
Salt River Project ("SRP")
Individual
David Grubbs
Ciy of Garland
No
Applicability: The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective: 4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3. Please state clearly the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
No
R1 - The auditors should be limited to verifying that a study was completed using the assumptions agreed to by both the TO and the reviewer. The auditor should accept any study and assumptions jointly agreed to by the TO and the reviewer without requiring additional engineering justifications as to why one type of study was used instead of the auditor’s preferred methodology. To summarize and echo FERC Commissioner Norris in his clarifying statement, included with the FERC Order that is the basis of the CIP-014 Standard, that if the Planning Studies indicate a transmission solution that would cause the substation to no longer cause the cascading outage that the transmission project could be initiated in lieu of the security plan. The additional transmission solution would potentially add other operational benefits other than just “security” and therefore may be more practical than the security plan in R4 through R6. In the guidance document, statements should be made that a TO may make additional planning studies at any time prior to the 30 months and if the third party reviewer concurs the updated study no longer shows a cascading event, whether due to changing grid conditions or system improvements, the standard would no longer apply including the continued implementation of the security plan. The TO should also notify the owner of the primary control center the substation no longer causes a cascading event. R2 - Timelines to complete third party verification under R2.2 and third party review under R6.2 are both too short. Increase 90 days to 120 days or 180 days. a. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A 90-day time limit may not provide sufficient time to conduct and verify a revised or supplemental BES assessment. b. For security reviews, conducting an accurate and meaningful review with sound recommendations applicable to a specific TPs facts and circumstances may require

additional time for assessment and discussions with the TO. A short review window is more likely to lead to misunderstandings, or disagreements with the TO which in turn could lead to discrepancies or improper application of the assessment requiring justification. This could cause the reviewer to avoid making recommendations that should be considered by the TO and improve the TO's assessment. c. As currently written, it appears if the TO disagrees with the reviewer's comments and writes a technical reason why he believes the original conclusion were correct, the recommendation(s) by the reviewer may be rejected and the TO's decision is final. Although I agree with this position it may be interpreted differently by the auditors. Please clarify which was the intent of the SDT. R3 - No comments
No
R4 - Sub requirement 4.1 should be modified to include specific language focusing the security study to those elements within the substation that can affect the reliability of the BES. The security plan should protect those elements of the substation as identified in the planning study in R1 that could cause the cascade or other unacceptable event identified in R1. Many substations identified in these studies are very large geographically and potentially very expensive to protect elements that may be located 30 to 50 feet above the ground. If these elements are determined to be critical they should be protected. If not, there is no justifiable reason to expend the resources to protect these devices. The security plans should concentrate on the protection of elements that could actually cause a cascading event, otherwise large expenditures may be made while adding no benefit or improvement to the reliability of the BES. R4.1 should read: 4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) including the identified elements within the station, substation or control center, that need to be protected that could initiate the cascading collapse identified by the planning study in R1; Under both R4 and R5 clarification should be provided to the auditors affirming that auditors do not need the work papers, or backup information used in preparing the security plan, it is preferable auditors be allowed to only view the plan on site and not be allowed to take a copy of the plan for their files due to the sensitive nature of the security plan. Having copies of the security plans of critical targets consolidated into the files of the auditing entity increases the security risk to the plan and identified assets do to a security beach or accidental release of the file. While having one security plan of a critical location is a security risk in and of itself, having a compilation of security plans by one entity becomes a national security risk. R5 - states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." The "and implement" should be deleted. It should be made clear the facilities, additional employees or other measure identified in the plan are not required to be in place at the end of the 120 days. The requirement should be clearly stated that a timeline needs to be developed as part of the plan and the TO and TOP will implement the plan per the timeline identified in the plan. The implementation may require several years to get through budget cycles, procurement, installation and implementation. R6 - The standard should make clear the auditor is not to audit the security plan for its content or appropriateness, but to confirm a security plan has been developed and that particular

security plan has been reviewed by a qualified entity. It should also be clear that a TO could expand its actual security beyond that identified in the approved/reviewed plan without requiring an additional review of such modification. Example: The original, approved plan had card readers on the doors and cameras within the yard. During the 30 months until the next required review, the TO added motion detectors as additional security measures at the substation even though they were not required in the initial security plan. The installation of additional monitoring or security measures beyond those in the approved plan should not initiate the need for a new security plan or third party review.
Yes
Definitions: primary control center - although not capitalized and therefore not a defined term, it is used in this standard in requirements 1, 3, 4, 5, and 6. The same term "primary control center" (again not capitalized) is used with a completely different meaning in standards EOP-008 in requirements 1.3, 1.5, 1.6, 2, 3, 4 and 7.1. Similarly "primary control room" is used in EOP-005 requirement 5 and in EOP-006 requirement 6 and is defined as the control center from which a TOP normally operates as opposed to the backup center. In CIP-014, it is defined/implied to be the control center that actually controls the circuit breakers at two or more substations. • If the term “primary control center” is used there will be confusion over the different meanings within the NERC Reliability Standards. • A completely different term should be used such as “primary local control center” or “primary transmission operations center”. The SDT apparently meant a "facility that has direct Supervisory Control". The term should be defined completely in the standard and should become a defined term within the Glossary of Terms used in NERC Reliability Standards. Proposed defined term: Primary Transmission Operations Center - One or more Transmission Owner or Transmission Operator facilities hosting operations personnel having primary operational real-time control of the BES elements in one or more remotely located substations using SCADA, EMS or other electronic means.” Please clarify whether these security plans are also required at any backup control center. Many of these control centers are generally not manned on a 24 by basis. unaffiliated - should be either defined or a footnote needs to be added to the Standard to explain that unaffiliated - means the selected verifying or reviewing entity cannot be a corporate affiliate, as stated in the guidance document. • Would two entities that do not have a direct ownership stake in each other but both are parties to an ownership in a third organization be considered to be unaffiliated? Example: Two utilities each have an ownership of a joint power plant but no ownership of each other. • What if they both had no ownership of the third party but both had purchase contracts with a third party? An explanation needs to be in the standard and not in the separate guidance document.
Individual
Michael P Moltane
ITC
Yes
ITC agrees with utilizing, as a starting point, the CIP-002-5.1 “medium impact” rating to determine the facilities needing enhanced physical security. As ITC indicated in its comments

to FERC in Docket No. RD14-6, these new physical security Standards must be developed in a coordinated manner to avoid duplicative, overlapping, or contradictory requirements among the various existing Reliability Standards that cover a similar if not an identical set of assets. By ensuring “that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1,” the SDT has fully met our expectations with respect to the applicability of the standard.
No
ITC believes that limiting physical security requirements in CIP-014-1 to those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection does not adequately raise the bar for critical infrastructure protection of valuable and strategic substation assets. Indeed, those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection certainly warrant additional physical protection. However, so does any other substation asset deemed critical through the cybersecurity initiatives already in place through applicable companion Reliability Standards. If a substation is deemed critical through the CIP-002-5 screening process, it at a minimum, should warrant an “evaluation of potential threats and vulnerabilities of a physical attack to the facilities (CIP-014-1 R4). ITC supports using the brightline test criteria of CIP-002-5, as noted in our comments for Question 1, above, but also feels that all substation assets passing the brightline test criteria should move directly to R4 for an assessment of threats and vulnerabilities, eliminating the need for R1 and R2. This has the benefit of using industry-vetted, bright-line criteria that creates valuable consistency between physical and cybersecurity assessment practices. This does not undermine the Commission’s three-part requirement for addressing physical security, but rather allows the responsible entity to meet the Commission’s first requirement (identification of critical assets) by using the same critical asset identification criteria for physical and cybersecurity. ITC believes if a facility is critical enough to warrant cybersecurity protection, then it should also warrant physical security and that the requirements should not be so narrowly defined to ignore the importance of substations beyond those few whose individual loss causes cascading outages. This simplified approach avoids potential contradictory and duplicative requirements between existing CIP standards, and would allow this standard to focus exclusively on physical security aspects and not on asset identification
Yes
Yes
Transmission systems tend to have facilities for which inoperability, while not causing immediate system failure or separation, would nonetheless leave the system in a degraded state. This degraded state will require system operators to reconfigure the system in a way to mitigate the loss of such facilities, but at that point, a new group of facilities could effectively become “critical” as that term is currently defined in CIP-014-1. For example, the loss of a given substation may cause several transformers to be inoperable, and with the long lead time for replacement components, the transmission owner would realistically need to plan for

the substation to be out of service for an extended period of time. During this time in which the substation is out of service, a second tier of assets may exist for which inoperability would now cause separation or failure of the type that would afford them a “critical” designation as currently defined under CIP-014-1. This condition would persist for as long as the original equipment was out of service. If the SDT were to adopt ITC’s proposed modifications to R1 (see above), this would not be an issue, since all CIP-002-5 substations would already be covered by CIP-014-1. However, if the SDT chooses not to adopt ITC’s proposal, the SDT should consider whether entities should assess the transmission system in this new degraded condition to determine if new critical assets are created due to the degraded condition (i.e., a reapplication of the analysis performed in the current R1 to determine if the loss of a particular substation causes widespread cascading.) The Standard could also trigger additional transmission system studies to determine if the transmission system remains reliable during the extended period in which the critical assets remain out of service.
Group
PPL NERC Registered Affiliates
Brent Ingebrigtson
Yes
These comments are submitted on behalf of the following PPL NERC Registered Affiliates: Louisville Gas and Electric Company and Kentucky Utilities Company; PPL Electric Utilities Corporation, PPL EnergyPlus, LLC; PPL Generation, LLC; PPL Susquehanna, LLC; and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP. The PPL NERC Registered Affiliates support the draft standard. As members of EEI, we also support the comments being submitted by EEI. In addition, we have provided specific comments that we believe would add clarity to the standards and simplify the requirements. We urge the SDT to consider our comments and incorporate them as appropriate when developing the final standard that will be balloted. Comments: Section 4.1.1.2 includes in the applicability Transmission Owners that own Transmission Facilities that are operating between 200kV and 499 kV at a single station or substation, where the station or substation is connected at 200kV or higher voltages to three or more other Transmission stations or substations and has an “aggregated weighted value” exceeding 3000 according to the table set forth in section 4.1.1.2. Because section 4.1.1.1 covers transmission facilities operated at 500 kV and above and section 4.1.1.2 only references Facilities operating between 200 kV and 499 kV, the fourth row in the table in section 4.1.1.2 referencing voltages of “500kV and above” is unnecessary and should be removed.
Yes
Requirement 1: 1. Requiring completion of an initial risk assessment for Transmission stations and substations planned to be in service within 24 months can lead to audit difficulties. Planned in service dates often change for a variety of internal or external reasons. It is requested that the SDT consider changing this language to a more easily identifiable trigger

such as requiring the risk assessment to be performed before a new Transmission station or substation is energized. 2. Does the R1 risk analysis require consideration of the impact of loss of lines with voltages below 200 kV in an identified Transmission station or substation? 3. It is unclear when the R.1 risk assessment needs to be completed. This should be clarified. 4. The wording in the Rationale for Requirement 1 box identifies the primary control center, but it also notes that control center electronic actions can cause direct physical actions at the Transmission station and substation. This would typically implicate the backup control center as well because the backup control center will have similar functional capabilities. There appears to be a disconnect between the use of the term primary control center and the parenthetical that follows which appears to include any control center that performs the listed functions.
Yes
Requirement 5: In the VSL table, does implemented mean complete execution of the plan including any necessary construction, or does it mean having initiated the plan but not necessarily completed all planned construction? There are only 10 days between VSLs. Requirement 6: 1. Similar to Requirement 2.3, the sub-requirements under Requirement 6.1 should be bullets, not individual sub-requirements. 2. Does R6 require subsequent third-party reviews when the security plan is revised? If so, what are the criteria?
Yes
We recommend that the SDT include a timeline within the standard which includes all required steps.
Individual
Eric Olson
Transmission Agency of Northern California
Agree
American Public Power Association
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Agree
American Public Power Association
Individual
Tony Eddleman
Nebraska Public Power District
No
Due to the imposed time constraints and expedited development of this standard, sufficient time isn't available to develop more realistic criteria for determining applicable substations creating unnecessary work and expense for transmission planners and reviewers.
No

The third party verification is unnecessary and should be deleted from the standard. There is no other unaffiliated third party that has knowledge and expertise comparable with the incumbent Transmission Planner who develops the detailed models, performs the reliability assessments, and develops the required long term plans for the Transmission Owner on an annual basis. If the verification remains in the standard, 90 calendar days is not a sufficient amount of time to complete verification. A Transmission Planner may ask a Planning Authority (PA) to review its risk assessments, but the same PA will likely be asked to review multiple utilities. Recommend at least 180 days to complete the verification.
Yes
Since we are using CIP-002-5 for identifying Transmission stations and substations, the confidential information for these facilities is already protected under CIP-011-1 Information Protection. CIP-014-1, requirements 2.4 and 6.4 are redundant with already approved requirements and are not needed. Adding requirements for protecting sensitive or confidential information in this standard will create confusion and double jeopardy. CIP-006-5 covers physical security and any information pertaining to the substations identified through the CIP-002-5 criteria. CIP-011-1 already protects this information. Due to the expedited development of this standard, sufficient time isn't available to provide clear requirements in the standard to evaluate compliance. The RSAW does contain language that will help, but the RSAW isn't the enforceable document and can be changed without industry approval. We've learned from implementing the other CIP standards that auditors can take a completely different position than what was meant by the drafting team with little recourse for utilities.
Group
GridWise Alliance
Ladeene Freimuth
Yes
Yes
Yes
Yes
GWA includes electric utilities, information and communications technology service and equipment providers, Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs), academic institutions, and energy consulting firms. GWA appreciates the acknowledgment in the Order of the significant efforts that industry already is undertaking to enhance the resilience of the electric grid and thereby protect the grid from a range of threats, including physical, cyber, natural, and other hazards. Industry has been working in close partnership with various levels of government to enhance grid protection, reliability, resilience, and security. This collaboration is ongoing and should be fostered for the

future. As you are aware, the electric grid is dynamic in nature. Electric grid owners and operators are making investments to enhance the reliability and resiliency of the grid, and are actively managing the operation of the grid to prevent outages and to restore power expeditiously, when outages do occur. As this process moves forward, GWA wants to underscore the importance that the result not be overly burdensome or inhibit innovation. It is important that the risk assessment process indeed be limited to truly "critical" infrastructure that is deemed essential to the functioning of the bulk electric system. This will help ensure that protection measures are reasonable and cost-effective, as well as cost-sensitive, to help minimize costs to industry and also to consumers, who ultimately must bear the costs of these investments. Industry is working hard to monitor and stay ahead of the myriad threats that could arise – physical, natural, cyber, and otherwise – recognizing that the types of threats and the motivations of potential actors continue to change over time. NERC should partner with FERC to ensure that an all-hazards approach to addressing risk is undertaken going forward. We appreciate the Order's acknowledgement of the vital need to protect confidential and sensitive information. Yet, we are concerned about the nature of information-sharing under this Order, and what protections and assurances, in fact, would be implemented to prevent the inappropriate sharing of confidential information. While also recognizing the need to protect the confidentiality of such sensitive information, we also note that it is important to ensure that information sharing is facilitated between the government and the private sector, as well as within the private sector. Vendors who supply critical systems and equipment are incorporated into this process, since continued coordination and cooperation among all the stakeholders is essential.
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
No
A) The FERC order directs that the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. It does not require verification of the specific or particular facilities identified. Therefore, SCE&G believes this section should be clarified and specifically state that the assessment itself (i.e. the methodology used by the owner or operator) be verified and not the facilities. B) SCE&G would like the drafting team to comment on the liabilities a NERC registered entity may assume as the third party when they are used to verify the risk assessment. Specifically, if in a future audit the owner or operator's assessment is found noncompliant, then would the independent NERC registered third party entity suffer any noncompliance as well? It is important for NERC registered entities to understand their compliance risks as third parties before they agree to perform independent verification of other entities assessments.
Yes

Yes
The requirement for unaffiliated third party verification throughout this standard is not consistent with other NERC Reliability Standard verification requirements. SCE&G is concerned that this standard sets precedence for future standard third party verification which would be very costly, confusing and burdensome.
Group
SERC CIPC
Cynthia Hill-Watson
Yes
Recommend that the drafting team include the Transmission Planner who would be performing the risk assessment in the applicability as discussed in R1.
No
Recommend that the Transmission Planner perform the risk assessment in R1 instead of the Transmission Owner. Need further clarification and examples for the term “unaffiliated”. Would “peer” reviews studies that do not have a single registered entity with controlling interest suffice as an “unaffiliated” third party reviewer? What role does the SDT envision the ERO (including regional entities) playing in the review process?
No
Recommend adding electric utility experience to 6.1.3 and 6.1.4. Consider removing the requirement for CPP and PSP certifications. Rationale: Numerous other mandatory enforceable standards (e.g. MTSA, CFATS, and CT-PATS) that do not require specific certifications nor are we aware of similar certifications in cyber elsewhere in the CIP standards. Suggest clarification of “electric utility experience” and “physical security experience” to allow the ERO and registered entities to justifiably select authorized third party reviewers.
Yes
Until the process of the standards has more fully matured there should not be a presecribed methodology for conducting the Security Vulnerability Assesments (SVAs) as long as generally accepted criteria as well as as stated in the standard in 4.1, 4.2, and 4.3 are followed in the development of the evaluation and plan(s). The comments expressed herein represent a consensus of the views of the above named members of the SERC CIPC only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Individual
William Temple
Northeast Utilities
Yes
Standard Drafting Team should define the term widespread. NU suggests the following definition: Widespread – An event that causes voltage collapse, Cascading and/or instability

that results in uncontrolled separation across significant portions of the Interconnection. The registered entity shall use regional criteria to evaluate.
Yes
Requirement 1 should match that language in the FERC order and not limit the assessment to Transmission System analysis and allow for an opportunity to apply technical expertise and judgment prior to the Transmission System analysis. We agree to Requirement 2 and Requirement 3.
Yes
Suggest standard allow entities to have a Master Physical Security Plan and that the standard provide for flexibility to accomplish mitigation activities associated with the results of vulnerability assessments and capture those under a separate mitigation plan (similar to the action plans associated to vulnerability assessments being conducted on Cyber Assets).
No
Group
Foundation for Resilient Societies
William R. Harris
No
1. Reliability Coordinators (RCs) would be exempted under the draft standard. Not all Reliability Coordinators are Transmission Operators or Owners. Peak Reliability, Midcontinent ISO, and Southwest Power Pool would be exempted because they are not in the NERC Compliance Registry as Transmission Operators or Owners. (MISO is not a Reliability Coordinator under its MRO registration.) The following standards apply to Reliability Coordinators but not Transmission Operators and Owners: Standard EOP-006-2 — "System Restoration Coordination"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies" (Applies to Balancing Authorities, Reliability Coordinators, and Load-Serving Entities); Standard IRO-009-1 — "Reliability Coordinator Actions to Operate Within IROLs"; Standard IRO-015-1 — "Notifications and Information Exchange Between Reliability Coordinators." The Joint U.S.-Canada report on the 2003 Blackout concluded that insufficient wide-area control, such as that provided by Reliability Coordinators, was a contributing factor to the blackout. Yet the Standard Drafting Team has disregarded these findings in exempting Reliability Coordinators. It is a fallacy to believe that only entities with direct control of substations need protection from physical attack. If critical substations and their Reliability Coordinators are attacked in a coordinated manner, what entity will lead system restoration? It is essential that Reliability Coordinators are designated as responsible entities, both to protect their own facilities and to enable their authority to review the adequacy of physical security capabilities for operating utilities in their coordinating areas. Key findings of the joint U.S.- Canada Outage Task Force on the August 2003 blackout demonstrated the need for the Reliability Coordinators to actively supervise operating entities both to meet essential operating needs and to assure adequate regional visibility. See U.S.-Canada Power System Outage Task Force

Report (April 2004). <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf> 2. Balancing Authorities would be exempted under the standard. According to the NERC Compliance Registry, there are 19 Balancing Authorities that are not also Transmission Operators or Owners. The following standards apply to Balancing Authorities but not to Transmission Operators or Owners: Standard BAL-001-2 — "Real Power Balancing Control Performance"; Standard BAL-002-1 — "Disturbance Control Performance"; Standard BAL-003-1 — "Frequency Response and Frequency Bias Setting"; Standard BAL-004-0 — "Time Error Correction"; Standard EOP-002-3.1 — "Capacity and Energy Emergencies"; Standard IRO-006-5 — "Reliability Coordination — Transmission Loading Relief". If critical substations and their Balancing Authorities are attacked in a coordinated manner, what entity will balance demand and generation and manage the emergency, especially if the attack causes a regional load imbalance? 3. Generator Operators would be exempted under the proposed standard. Generator Operators have vulnerable and hard-to-replace Generator Step Up (GSU) Transformers, just as Transmission Operators have these transformers. Generation facilities could present contingencies in excess of spinning reserves, especially in congested areas with import of large megawatts of power over long transmission lines. Hence, Generator Operators should be included in mandatory physical security protection standards. 4. The standard does not require modeled contingency planning for scenarios of physical attack. Contingency planning for physical attack should include megawatt capacity of all generators at single generation facility, not just failure of some individual units at the facility. 5. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard. Physical attack of multiple transformers is different than the random failures planned for under the standard N-1 criterion. We have already seen attack on multiple transformers and their circuits at the Metcalf substation. The standard's criterion for violation of IROL limits would not be valid if the IROL limits assume random failures rather than coordinated physical attack. 6. Some "High Impact" control centers would be exempt under the standard. Examples include the control centers for Peak Reliability, MISO, and SPP. In all, these control centers manage power for 141 million Americans. Control centers for Reliability Coordinators, Balancing Authorities, and Generator Operators are included in the "High Impact" Criteria for CIP-002-5.1 How can the standard drafting team take the CIP-002-5.1 criteria for substations but not control centers of Reliability Coordinators, Balancing Authorities, and Generator Operators? FERC Directive RD14-6-000 specifically requires protection of critical control centers in Footnote 6: "… the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers." 7. While FERC Directive RD14-6-000 [146 FERC ¶61,166] did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Such measures might include: Opaque Fencing; Concrete Jersey Barriers; Motion Sensors; License Plate Scanners; Intentional Electromagnetic Interference (IEMI) Detectors; Gunfire Locators; Limiting of Close Public Access, Including Recreational Access; Armed Private Guards; Police Details; Deployment of National Guard

Troops; Better Stocking of Spares—e.g., Transformer Bushings and Radiators; Equipment Monitoring and Redundant Telemetry to Control Centers. Instead, the standard relies upon self-devised security measures without prioritization or other guidance. 8. The Metcalf incident unambiguously showed the value of equipment monitoring in mitigating physical attack on power transformers. Gunfire locators, had they been installed at Metcalf, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement. Intentional Electromagnetic Interference (IEMI) Detectors could likewise provide real-time warning. If threat sensors with reliable and cyber-protected alerts are not part of a physical security system, it will be impossible to mobilize time-urgent countermeasures and impractical to take precautionary measures at other at-risk facilities vulnerable to coordinated attack. 9. Intentional Electromagnetic Interference should be a physical threat included in the standard, because IEMI attack could occur in the physical proximity of facilities and could cause permanent physical damage in additional to temporary upset. IEMI detectors are a cost-effective measure as these devices cost approximately $15,000 per unit. 10. The Metcalf Incident was both a physical attack and a cyber denial-of-service attack. The need for linkage between physical and cyber is explicitly called for in the RD14-6-000 Order of March 7, 2014, para 5, footnote 3. The implementation plan under this Order must require responsible entities to identify and protect cyber assets that link facilities and control centers that are otherwise identified as critical to the reliability of the BES. Communications and Network entities routinely provide hardened and alternate routing for military, other government and the Defense Industrial Base and their services should be an explicit requirement for Physical Security Standards that apply to any units and control centers that are identified by Responsible Entities as critical to the Reliability of the BES. 11. Review and certification of security plans, as proposed in the draft standard, does not necessarily provide a level of independence that would be prudent or credible to the public. Regional Entities or Reliability Coordinators for any facilities under their jurisdiction should be the primary authorities to review and approve security plans. Governmental authorities should have the ability to audit security plans. 12. Improvements to the standard that we suggest would be marginal additions of facilities and their equipment and therefore would be cost-effective. We propose inclusion of primary and backup control centers for Peak Reliability, MISO, and SPP—an increase of 6 control centers as compared to approximately 200 already included Transmission Operator control centers. We propose inclusion of 19 additional Balancing Authorities as compared to 114 Balancing Authorities in total. There are only 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more—this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked. 13. RD14-6-000 directs NERC to submit for approval a physical security standard that would apply to the most critical facilities of the Bulk Electric System. The Standard Drafting Team has narrowly interpreted “critical facilities” to mean transmission facilities and directly linked control centers. We disagree with this narrow interpretation. Given the NERC interpretation and the 90 day deadline for standard development, NERC’s draft standard holds tightly to the most minimal facilities and therefore has significant gaps in protection as we describe in our foregoing comments. Some of these gaps, such as the exemption of Reliability Coordinators

and Balancing Authorities, are so fundamental that they should be addressed immediately. For other gaps, we ask that NERC open a Standard Authorization Request (SAR) for a Phase Two physical security standard. This follow-on Phase Two standard should require modeling of BES operations sufficient to ensure identification of facilities that could cause cascading outage, single points of failure, data connectivity needs, and other processes and technologies essential to grid protection—in short, a standard designated CIP-014 Version 2. An approved SAR for a Phase Two standard should be concurrent with NERC Board of Trustees approval of the current standard in development.
No
Same answer as provided to Question 1.
No
The third party review is not adequately specified. The Joint U.S.-Canada Outage Tasf Force Report (April 2004) determined that lack of Reliability Coordinator oversight, and legal authority, contributed to inadequate supervision of transmission operators, and reduced visibility of regional inadequacies. See our comment to Question 1 for our view that Reliability Coordinators and Balancing Authorities must be involved.
Yes
We recognize that FERC has established a 90-day review process, and that NERC has worked to meet the tight deadline. Hence, the Foundation for Resilient Societies asks NERC to develop a SAR for Physical Security Standards - Phase 2. In this process, analytical modeling should be undertaken to identify and prioritize physical security risks that include cyber vulnerabilities, and that relate to the need for reliable warning and communications via redundant channels to control centers and to law enforcement. It should not be acceptable to exclude Regional Coordinators and Balancing Authorities, both groups needing to review and perhaps upgrade their own physical security, and both groups playing key roles in oversight of the operating entities, both TOs and GOs, whose physical security may be essential to prevent long-term outages through coordinated attacks. For additional materials prepared by the Foundation for Resilient Societies, contact the FERC staff designated to assist NERC with standard setting in FERC Docket RD14-6-000.
Individual
Guy Andrews
Georgia System Operations Corporation
No
Georgia System Operations Corporation (GSOC) appreciates all the effort going into the draft of CIP-014-1 Physical Security Reliability Standard. GSOC supports the comments submitted by NRECA.
No
GSOC supports the comments submitted by both Georgia Transmission Corporation (GTC) and NRECA
No

• GSOC supports the comments submitted by both GTC and NRECA. • In addition, GSOC suggests in R4.2 changing “Prior history or attacks on” to Prior history of physical security related events at” to better describe the subrequirement. • GSOC suggests in R6, last sentence, changing the word “development” to “developed” in order to be consistent with the word “performed” in the same sentence.
Yes
GSOC supports the comments submitted by NRECA
Individual
David Godfrey
Texas Municipal Power Agency
Agree
City of Garland and American Public Power Assocation
Group
Bureau of Reclamation
Erika Doot
No
The Bureau of Reclamation (Reclamation) believes that the Transmission Planner, Planning Coordinator, and Reliability Coordinator should be included in the Applicability section of the standard and should be responsible for reviewing the Transmission Owner’s risk assessment (BES impact assessment).
No
Reclamation agrees with this approach. However, to promote consistent identification of critical facilities within an interconnection, Reclamation believes that the third-party review should be conducted by the Transmission Owner (TO)’s Planning Coordinator or Transmission Planner. If the Transmission Owner is also the Transmission Planner and Planning Coordinator, the third-party review should be performed by the Reliability Coordinator. Reclamation also suggests that the drafting team modify the term “risk assessment” to “BES impact assessment.” In the physical security community, the term “risk assessment” generally refers to “The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.” See ASIS International, General Security Risk Assesment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term “BES impact assessment” so it is clear that the initial evaluation is of risk to the BES if the substation is rendered inoperable or damaged. Reclamation also recommends revising R1.1 to require subsequent risk assessments every 60 months for all Transmission Owners. Reclamation believes that periodic risk assessments are necessary, but has not seen evidence that the costs associated with updating risk assessments every 30 months rather than every 60 months would provide commensurate reliability benefits. Reclamation recommends that the drafting team update R1.1 to state, “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged

could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.”
No
Reclamation agrees with the requirements to develop a threat assessment and physical security plan. Reclamation also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers. However, Reclamation does not believe that the proposed requirements will allow adequate time for a comprehensive review. Reclamation suggests that at least 180 days would be a more appropriate timeframe for a detailed threat analysis and physical security plan review. Reclamation also requests that the drafting team clarify the scope of third party reviews of these threat assesments and physical security plans, perhaps by adding additional detail to the Guidance and Technical Basis section. Reclamation is not convinced that third-party reviews will increase reliability. Reclamation believes that each entity is in the best position to evaultate threats to its facilities and determine appropriate mitigation plans. Reclamation is concerned that the well-intentioned third-party review mandated by the order could result in classified or national security related information falling into the wrong hands. Reclamation does not believe that non-disclosure agreements will adequately protect this sensitive information.Reclamation believes that audits by regional entities in essence provide a “third-party” review of an entity’s threat assessments and physical security plans.
Yes
Reclamation is concerned that the term “primary control center” will become confused with the NERC Glossary term “Control Center.” As indicated by the use of the term “monitor” in the definition of Control Center, Reclamation does not believe that the concept of “operational control” has been equated with “causing direct physical action” to date. To avoid confusion, Reclamation suggests that the drafting team replace the R1 phrase “primary control center that operationally controls eachTransmission station or Transmission substation” with the phrase “primary control center that physically controls each Transmission station or Transmission substation.”
Individual
David Revill
Georgia Transmission Corporation
No
Georgia Transmission Corporation (GTC) supports the efforts of the drafting team and believes that their efforts to create the CIP-014 Standard are moving in the right direction. GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.
No
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. -GTC is concerned that the language of the standard and rationale around the use of the term “unaffiliated” in R2 and R6 does not

provide sufficient clarity for a registered entity to have confidence in the consistent applicability and auditability of the requirement. GTC suggests additional examples or requirement language to consider whether: -entities that are not under the same corporate parent but which have contractual obligations between each other would be considered “unaffiliated” - organizations or teams made up of representatives of multiple utilities with no one utility having a controlling interest in the findings of the group would be considered “unaffiliated”
No
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. - GTC requests revision to the requirement language or addition of guidance around the phrasing of “unique characteristics” in R4 to address whether all equipment within an identified substation has to be assessed in R4 or if an entity has the option to focus their threat and vulnerability assessment on specific facilities in the substation which were identified as causing the adverse effects described in R1. -GTC is concerned that the language of the standard and rationale around the use of the term “unaffiliated” in R2 and R6 does not provide sufficient clarity for a registered entity to have confidence in the consistent applicability and auditability of the requirement. GTC suggests additional examples or requirement language to consider whether: -entities that are not under the same corporate parent but which have contractual obligations between each other would be considered “unaffiliated” - organizations or teams made up of representatives of multiple utilities with no one utility having a controlling interest in the findings of the group would be considered “unaffiliated”
Yes
-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard. -GTC suggests that in M2 the word “communications” be changed to “notifications” to follow the language of the requirement. -GTC suggests that in M2 and M6 the measures should be updated to include evidence of the qualifications and independence of the respective review teams. -GTC suggests that M6 the measures should be updated to include evidence of the implementation of procedures for information protection used during the third-party review.
Individual
Scott Langston
City of Tallahassee
Agree
APPA
Individual
Bernard Johnson
Oglethorpe Power Corporation
Agree
Georgia Transmission Corporation (GTC) National Rural Electric Cooperative Association (NRECA)

Group
National Grid
Michael Jones
Yes
It should be clear that the applicability section of the standard is only intended to provide a valid, technically sound basis to be used as the ‘starting point’ to those transmission facilities or stations that should be included in the risk assessment. We suggest the following modifications: 4.0 Applicability: 4.1 Functional Entities: 4.1.1 Transmission Owner that owns any facilities identified in the following sections (4.1.1.1 through 4.1.1.4) will be required to perform the risk assessment and risk assessment validation as outlined in R1 and R2 of this standard. Should the risk assessment identify critical assets then the Transmission Owner is subject to the remaining requirements (R3 through R6) of the standard. 4.1.2 Transmission Operator
No
While we support using the CIP-002-5.1 criteria as a starting point for applicability of the draft standard, we do have concerns with the inclusion of the phrase “within an Interconnection” in R1. FERC Order RD14-6 directs that "[a] critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System". By introducing the word “within,” the Standard could inadvertently draw widely different interpretations of how to assess risks to the BPS. In practice, this could open up the potential for the inclusion of regional or localized transmission impacts, which we believe is in contrast with the Commission intended scope in the Order. As a result, we suggest that the wording in R1 be modified to the following: “A critical facility is one that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation or cascading failures widespread across significant portions of an Interconnection". Alternatively, we recommend clarifying in the guidance documents that ‘widespread’ and ‘within an Interconnection’ proposed words are intended to apply to impacts to the BPS that reaches deep into the Interconnection, and not affecting a small portion of an Interconnection. For example, if an Interconnection has relatively small Balancing Authorities (BAs), ‘widespread’ would need to be interpreted as impacts that would be crossing several, i.e. more than two, of those BAs in order to be considered ‘widespread’.
Yes
No
Individual
Donna Johnson
Oglethorpe Power Corporation
Agree

Georgia Transmission Corporation (GTC) National Rural Electric Cooperative Association (NRECA)
Individual
Joshua Andersen
Salt River Project
Yes
SRP supports comments submitted by APPA.
No
SRP supports comments submitted by APPA with the following additions: The time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. If possible, could the drafting team revise the language of Requirement R1 to make this clear? The periodicity of the risk assessments required by Requirement 1 and the time frame that the risk assessments appear to not align. The risk assessment is required to include Transmission stations and Transmission substations that exist as well as those planned to be in service within 24 months. However, the periodicity for conducting future risk assessments is every 30 calendar months or every 60 calendar months if the prior risk assessment did not identify any Transmission stations or Transmission substations. This potentially leaves a gap of six to 36 months where facilities may not have been assessed. In R2 it is not clear that the primary control center must also be verified, but in subsequent requirements it implies or states that it should be. If the intent in R2 is that the primary control center should also be verified, then it should state so in R2.2 and R2.3 in addition to stating stations and substations. Third Party Verifiers: SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated

with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
No
SRP supports comments submitted by APPA with the following additions: Third Party Verifiers: SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different

in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities. Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers. Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Yes
Section C “Compliance” 1.4 (page 13) which states “...all evidence will be retained at the TO and TOP facilities.” is contradictory with NERC Compliance Monitoring and Enforcement practices which allow data to be exchanged with and sent to Regional Entities such as in pre-Audit data requests and Mitigation Plans. In addition, this would be burdensome for the TO/TOP because the 3rd party verifying/reviewing entities would need to be on-site and potentially incur travel expense.
Individual
Patrick Farrell
Southern California Edison Company
Yes
No
SCE has concerns with both Requirement R1 and Requirement R3. In Requirement R1, SCE recommends that the verbiage be changed from “…that if rendered inoperable or damaged could result in widespread instability...” to “...that if damaged to the point of being rendered inoperable could result in widespread instability..." SCE requests this change to reduce ambiguity in the application of the word "damaged." In addition, language should be added to R1 that specifies: “…system instability such as uncontrolled separation or cascading within 15 minutes of compromise…,” as a 15-minute window would align with criteria in the CIP standards used to determine critical facilities. In the guidance section for R1, SCE would suggest changing the text from “…remedial action schemes (RAS) or special protection

systems (SPS)" to "…special protection systems (SPS)…," because as used in the NERC Glossary of Terms, a RAS is included as a type of SPS. In addition, SCE requests that R1 be revised to include specific examples and criteria for the risks to be measured. For instance, SCE believes the following could be among the examples and criteria specifically included: (a) Thermal overloads beyond facility emergency ratings; (b) Voltage deviation exceeding ± 10%; (c) Cascading outage/Voltage collapse; and (d) Frequency below under-frequency load shed points. With respect to Requirement R3, SCE requests that additional guidance be provided on how a "primary control center" should be identified, as that term in used in both Requirements R1.2 and R3. SCE also asks the team to consider changing the notification requirement in R3 from seven(7) to thirty(30) days in order to allow sufficient time for the transmission owner and transmission operator to perform the required communication.
No
SCE has concerns with Requirements R4, R5, and R6 that will be described below. With respect to Requirement R4, SCE notes that entities are required to "…conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)…" SCE requests the inclusion of additional guidance or examples of threats and potential vulnerabilities that an entity may want to consider. This will allow entities to perform a threat assessment and develop preventative measures that are commensurate with the intent of the standard. In addition, SCE requests additional guidance on physical security plans that allow for flexibility to deal with emergent threats. With respect to Requirement R5, SCE believes that in the guidance section, the drafting team should consider referencing standards that are used by security professionals or organizations, in order to ensure that the criteria to identify appropriate countermeasures to potential threats and physical attacks are evaluated along similar themes across industry. SCE also requests that the team consider rephrasing R5.1 from "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond…" to describe the control, to "…deter, detect and delay, and also assess, communicate, and respond…" With respect to Requirement R6, SCE requests that the team consider rewording Requirement R6.1 from "Each Transmission Owner and Transmission Operator…" to "Each Transmission Owner or Transmission Operator, with facilities identified as a result of R2,…"
No
Individual
John Hagen
Pacific Gas and Electric Company
Yes
Yes

R2 Comment: Suggest removal of the requirement for a third party risk assessment verification. Verifications already occur as part of internal compliance programs in CIP-002 and when audited by the Region. What if the assessment is performed by a third party, do you have to get another third party to verify? This creates a significant administrative burden, even if the Standard will only apply to a small number of entities and facilities. R3 (pg. 8) "…the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify…" Comment: Seven calendar days may be too short a time requirement, consider 10-14 days
Yes
R4 (pg. 9) "…shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)…" Comment: Consider stating "…conduct a physical security risk assessment to identify and evaluate potential threats and vulnerabilities…" The assessment should identify the potential threats and vulnerabilities to evaluate and implement the necessary protective, detective and corrective countermeasures R5 (pg. 10) states to develop and implement a documented security plan (s) within 120 calendar days of completion of R2 (unaffiliated third party verify the risk assessment form R1). Furthermore, R5.1 states to address the potential threats and vulnerabilities from R4. 120 days to implement the countermeasures may not be enough time (logistics, procurement, installation timelines, approvals, etc.). Comment: Could they say "…shall develop and begin implementation of a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days…" because in R5.3 it requires a timeline for implementing the enhancements. 6.1.1. (pg.11) "An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification." Comment: Shouldn't require a specific certification, should say something like "The third party must include in their review the qualifications of the staff performing the review." R6.1.2 (pg. 11) "An entity or organization approved by the ERO." Comment: What criteria is the ERO using to approve entities or organizations? The approval process needs to be spelled out. R6.1.3 (pg. 11) "An entity or organization with demonstrated law enforcement, government, or military physical security expertise" Comment: Does this mean we can use Law Enforcement agencies or firms with retired law enforcement personnel?
Yes
Compliance 1.2 (pg. 13) Comment: can they clarify by being less wordy and just start by saying "The responsible entities shall retain documentation as evidence for three years", followed by the rest in less words?
Group
ISO/RTO Standards Review Committee
Greg Campoli
Yes

Introduction The proposed standard provides adequate flexibility with respect to the risk assessments and security evaluations and plans. This allows the industry to capitalize on their experience in these matters, while also accommodating changes that warrant consideration. Applicability Section The applicability scope is reasonable in terms of identifying the appropriate functional entities to address physical security concerns. Similarly, the proposed standard establishes a reasonable approach for identifying the scope of facilities by 1) initially defining an objective set based on the CIP-002-5.1 criteria, and then 2) refining that set based on analyses that assess the relationship of those facilities to specific, system conditions/impacts metrics – i.e. widespread instability, uncontrolled separation, or Cascading within an Interconnection.
Yes
R1 R1 in conjunctions with the Applicability section is a reasonable approach for identifying the scope of facilities subject to R2 – R6. R2 Imposing a verification requirement is a reasonable way to facilitate an effective outcome in terms of identifying facilities that meet the impact thresholds established in R1. Requiring the use of an unaffiliated third party is reasonable because it mitigates the potential for inadvertent error in study work. Finally, allowing the verification to occur concurrently or subsequently, and leaving that decision to the discretion of the relevant functional entities, is appropriate. The functional entities should have the discretion to determine the most effective means of performing the verification. R2.1 requires that the verifying entity be either 1) a registered RC, PC or TP, or 2) another entity with appropriate planning or analysis experience. This is a reasonable approach that provides appropriate flexibility with respect to third party verification options. It also addresses the different operational and planning structures that comprise the North American electric grid – i.e. organized market regions where different entities can perform the different NERC registered functional roles (ISOs/RTOs) and vertically integrated regions where all the relevant roles under the standard may be performed by a single entity and, therefore, would require the use of an independent third party to perform the unaffiliated verification. R2.2 requires the third party verification to either confirm the TO analysis under R1, or, alternatively, recommend that facilities be added or deleted (the IRC assumes that a verification can confirm some results and also add facilties or remove facilities). Although R2.2 establishes a reasonable standard – i.e. verify TO results or recommend changes - the IRC offers the following comments. The requirement, as written, imposes the obligation on the third party verifying entity. However, the TO is the responsible entity under the standard – i.e. the TO is required to obtain the third party verification. The language should be revised to clarify that the relevant actionable obligation (to obtain the third party verification) lies with the TO. The next issue raised by R2.2 is the timing. The IRC appreciates the importance of the issues being addressed by the proposed standard and the goal of implementing the standard and the relevant processes contained therein in a timely fashion. However, practically speaking, 90 days may be difficult to meet depending on the number of Transmission Owners that require verification from a single Registered Entity. For example, in organized markets there may be numerous TOs all selecting their PC to verify. To the extent implicated in reviews under the standard, IRC members would make best efforts to perform any relevant verifications. This comment is merely intended to highlight the potential resource impacts

under the proposed 90 day timeline. The IRC proposes the following revisions to mitigate the issues in R2.2 described above. 2.2. The third party verification shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within a mutually agreed upon timeframe between the Transmission Owner and the third party but no longer than 180 calendar days following the completion of the Requirement R1 risk assessment. R3 R3 obligates the TO to notify a TOP that has operational control of a control center associated with a facility identified pursuant R1 and verified under R2. R3.1 requires similar notification if a facility is removed via those processes. The standard may benefit from including the draft guidance into the R3 rationale section that clarifies that operational control means the ability to take action that affects the physical status of the facility, and that it does not include directive control, which relies upon another entity to take operational action to change the status of the facility. The guidance document addresses this issue, but the SDT could add clarifying language to the rationale section of R3, similar to the language in the guidance document and/or the language in the R1 rationale section, which reads in relevant part: "… identify the primary control center that operationally controls that Transmission station or Transmission substation (i.e., the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity)."
The IRC has no comments on R4-R6.
No
Group
APPA
Paul Haase
Agree
The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities, physical infrastructure, including risk assessments

and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language (new subrequirements): R1 1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3 3.4 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under Requirement R1 of this standard. R4 4.1 The Transmission Owner will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 conducted under this standard.
Individual
David Francis
MISO
Yes
MISO supports the proposed applicability section and agrees that other entities do not need to be included. In particular, MISO would not support application of this Standard to Reliability Coordinators or Balancing Authorities, as these entities' control centers are adequately protected with regard to physicial security under CIP-006-3c and its successor standard. Moreover, these control centers are subject to the requirements of EOP-008-1 including the transfer functional control to backup facilities. MISO therefore agrees that the focus of CIP-014-1 should be those facilities that are not otherwise fully protected by CIP-006-3c, such as those that do not not rely entirely on Critical Cyber Assets to maintain reliability.
No
MISO recognizes that the Commission mandated third-party verification of the risk assessment required under R1, however the current language of R2 requires modification to address several concerns MISO has with regard to its potential role as a verifying entity. While MISO has every confidence that it can perform risk assessment verifications in a safe, responsible, and accurate manner, the combination of a high number of requests requiring

verification within a relatively short period of time presents some concerns to MISO regarding its resource allocation and availability. In particular, MISO recommends that the SDT add language limiting the universe of Transmission Owners/Operators that can seek verification from a particular verifying entity (potentially by geographical region or contractual or functional relationship) as well as modify the 90 day requirement to take into account that a single entity may have more requests than it can feasibly complete in such a short time period. An example of language that MISO could support is language that would allow a verifying entity and the requesting Transmission Owners/Operators to agree upon an appropriate completion date beyond the 90 days where the 90 day period will not allow completion of a robust verification due to resource constraints by the berifying entity. Finally, MISO respectfully requests that the SDT consider adding language to Requirement R2 that would allow verifying entities to limit liability related to both enforcement actions within the jurisdiction of FERC, NERC, and the Regional Entities and other actions that could be brought against verifying entities in other jurisdictions and venues unless it is shown that the entity lacked good faith or was grossly negligent.
Yes
No
Individual
Sergio Banuelos
Tri-State Generation and Transmission Association, Inc.
No
The drafting team may want to consider language referencing the CIP-002 Critereon rather than outright copying it in order to prevent changing multiple standards as the CIP-002 standard evolves. CIP-002-5.1 Attachment 1: Overall Application gave guidance on how to treat joint ownership facilities. Tri-State feels that this new standard would also benefit from such guidance.
No
Rather than making it the Responsible Entity’s responsibility to find a third party to verify its assessment, Tri-State believes it would better suit the industry and the standard if R2 required either the Reliability Coordinator or Regional Entity to request TO's assessments on an intervaled basis. This meets the requirements of the March 7 FERC Order. Allowing the requirement to be broad enough to allow third party paid consultants with “transmission planning or analysis experience” creates a conflict of interest and contradicts the draft standard’s requirements for the use of “unaffiliated third part[ies]”. If third party – other than NERC or the RE – verification of the assessment is required by the standard, then this is effectively two audits (and two 3rd party assessments) on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the

standard is currently drafted. Tri-State recommends that rather than 30 months and 60 month risk assessment intervals for R1.1, they should be a more straightforward 36 months and 72 months respectfully in order to be consistent withnormal auditing time periods of three years. This will make the intervals easier to track with internal programs and controls.
No
Tri-State disagrees that the FERC order specifically forces the drafting team to have a requirement for 3rd party verification. The order uses the word “should,” not “shall” or “require.” Tri-State would argue that 3rd party verification would/will occur during scheduled audit times. Again if the drafting team feels a need to require an additional 3rd party verification, it should require the Regional Entity or Reliability Coordinator to request the plans.
Yes
While the FERC Order RD14-6 paragraph 13 does require NERC to file a proposed standard within 90 days, footnote 8 only requires that the proposed standard include timelines for certain elements, without specificity for what those timeframes should be. The bright line CIP version 5 applicability that is used within this standard became effective 02-03-14 and was giving industry 24 months to implement. The CIP-014 draft appears to assume those bright line considerations are already completed for industry and provides just over 6 months to complete an additional assessment to remain compliant. Without specific implementation timeframes provided by FERC, and to stay in closer alignment to the expected completion dates for CIP v5, Tri-State is recommending no less than a one year after this standard becomes effective for the R1 risk assessment to be completed.
Group
California Public Utilities Commission: Safety and Enforcenment Division
Raymond G. Fugere
Agree
California Public Utilities Commission Safety and Enforcenment Division
Group
Bonneville Power Administration
Andrea Jessup
Yes
4. Applicability: BPA believes that the medium list for HV transmission entities will result in numerous facilities having to be protected (all 500 kV) contrary to the drafting team comment that not many facilities will be deemed critical. 4.1. Functional Entities: BPA recommends that this section reference the criteria of CIP-002-5.1 for a “medium impact rating,” instead of re-stating it without citation. Otherwise it is confusing. For example, the source of the tabulated weighting criteria is unclear and it is difficult to know there is a connection to any previous or established standards.
No

R1 Terminology: Although the term “risk assessment” in this section is in alignment with language in the FERC order, BPA recommends that it be revised to consequence or impact assessment. This is a physical security standard, and the term risk assessment should be reserved for the physical security risk section of this standard and align with security industry use of the term. BPA believes the basic intent of R1 is to identify substation facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection can create unacceptable consequences to the BES and not to assess risk of the event happening. Also, BPA suggests that additional sub-requirements be added to provide clarity on what system conditions and performance criteria or methodology need to be considered in order to determine what stations and substations will be deemed critical. Similar language found in existing standards would be helpful. Examples: FAC-010-2.1 (System Operating Limits Methodology for the Planning Horizon), R1-R3; FAC-013-2 (Assessment of Transfer Capability in the Near-Term Planning Horizon), R1; TPL-001-4 (Transmission System Planning Performance Requirements), R1-R6; TPL-004-0a (System Performance Following Extreme BES Events), R1. "R1 1.1. Subsequent risk assessments shall be performed:" BPA recommends revising R1 1.1 to: “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.” Justification: This would consolidate the two bulleted actions and make them equally applicable. BPA has been doing substation facility impact and security risk assessments for the past 15 years and our experience is that the criticality of a substation facility does not change once ranked; once it is determined critical it will always be critical particularly when information is used in a physical security risk assessment. A 5 year interval would be a more appropriate interval for this type of assessment as it would always be case of identifying new facilities and not excluding ones previously identified. "R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R2 first sentence to: "R2 Each Transmission Owner shall verify the impact assessment performed under requirement R1 by a third party entity other than the owner or operator." Justification: This fully aligns with the requirements of the FERC order by using the requirements of the FERC order. BPA believes the introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of an impact assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes that the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft “unaffiliated” is especially troublesome for federal government-owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the federal government

transmission owner. Also, BPA believes industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into widespread use. Please note that the FERC order only recommends this verification as it is stated as “should” and not as “shall.” "R.3 For a primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. [VRF: Lower; Time- Horizon: Long-term Planning]" BPA recommends revising the 7 day requirement in R3 and R3 3.1 to 30 calendar days. Justification: This information is not that time critical at this stage, and one week will not be enough time to complete all notifications.

No

R4. BPA agrees with the requirements to develop a threat assessment and physical security plan. BPA also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers as noted in R6 (Section R6.1.3.) However, BPA requests that the drafting team clarify the scope and purpose of third party reviews should they remain as part of the standard. BPA disagrees that third party reviews will increase reliability and notes the draft standard exceeds the scope of the FERC order Paragraph 11. BPA believes that each entity is in the best position to evaluate threats to its facilities and determine appropriate mitigation plans. Nonetheless if third review is deemed necessary, BPA believes that it should be allowed to have another federal agency perform its third party review. In other words, for purposes of this standard, another federal agency would be deemed to be “unaffiliated” with BPA. Keeping this information within the federal government will decrease the risk of inappropriate disclosure of such information. BPA believes that non-disclosure agreements with non-federal parties may be a poor substitute for this because they can only be enforced once a disclosure is made. At that point, it is often too late and the information is available to a wider audience than intended. "R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator’s primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: [VRF: High; Time-Horizon: Long-term Planning]" BPA recommends revising the 120 day requirement in R5 to 12 calendar months. Justification: This information is important to get right as security designs and enhancements will be built from this plan. 120 days is not be enough time to develop a complete and effective security plan

and incorporate finalized threat assessments. "R6 Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R6 first sentence to: "R6 Each Transmission Owner shall verify the risk assessment performed under requirement R4 by a third party entity other than the owner or operator." Justification: BPA believes the proposed revision fully aligns with the requirements of the FERC order by using the requirements of the FERC order. The introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of a risk assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft "unaffiliated" is especially troublesome for federal government owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the government transmission owner. Also, industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into wide spread use. Please note that the FERC order only recommends this verification as it is stated as "should" and not as "shall."

Yes

The current draft requiring "unaffiliated" third party review is more restrictive than the requirements language in the FERC order and meeting an unaffiliated requirement will be problematic for federally owned power and transmission systems. Paragraph 8 of the order: "Thus, the Reliability Standards should require the owners or operator to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process." BPA's interpretation of the FERC order is that consultation with peer entities would be acceptable methods for review of evaluation processes. In fact the order by its wording encourages such consultations without restriction as to business or corporate relationships. The draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities

corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The “unaffiliated” requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term “unaffiliated” and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard. Paragraph 11 of the FERC order: “In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity.” BPA believes the draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The “unaffiliated” requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term “unaffiliated” and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard.

Group

California Public Utilities Commission: Safety and Enforcenment Division

Raymond Fugere

No comments

In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive. The use of unaffiliated verifying experts is a positive element in the draft standard. In general, the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3, second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. With respect to Rule R1, Section 1.1, the drafting group should consider whether there should be language added to the standard detailing a process whereby the 30 or 60 month intervals should be accelerated in the event of serious intervening situations. With respect to Rule R2, Section 2.1, the description of “an entity that has transmission planning or analysis experience” is overly vague and should be further clarified, or that the use of this type of expert should be limited to certain small transmission owners. With respect to Rule R2, section 2.4, the language requiring “non-disclosure” agreements is important and a positive element in the draft standard.

In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive. The use of unaffiliated verifying experts is a positive element in the draft standard. In general, we believe that the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3,

second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. Section 5.1 of the draft refers to “resiliency”. Does this term refers to actions such as building redundancy or improving protective schemes, as opposed to direct physical protection activities? The standard should clarify the meaning of the term resiliency. Section 4.1 of the draft refers to “unique characteristics.” Assuming this consideration includes availability of spares and ease of repair, the language is acceptable. With respect to Rule 5, section 5.2, the drafting group should consider language requiring the security plan to include contact and coordinating information for other utilities or important stakeholders, in addition to law enforcement. With respect to Rule R6, section 6.4 the language requiring “non-disclosure” agreements is important and a positive element in the draft standard. Section 4.2 lists the elements to be considered in evaluating the potential threats and vulnerabilities to physical attack, and specifically states "[p]rior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events and ...". We suggest that in additional to geographic proximity, that the section add language concerning "similarity of geographic characteristics". While geographic proximity, is a factor, ease of accessibility, layout and geographic contour, of an attacked facility is also important, if not more so.
Individual
Glen Sutton
ATCO Electric
Yes
No Comment.
Yes
Although the FERC order contains language that a third party verification occur, this type of verification is not used anywhere else in NERC reliability standards for similar activities (e.g. CIP-002 classification). ATCO Electric (AET)respectfully requests that the review be allowed to be performed by qualified in-house Engineering groups who already perform these functions. Mandating a third party verification presents a risk to timelines and the implementation of the other requirements.
Yes
AET agrees with the flexible approach outlined by the draft standard and respectfully offers these following comment for the drafting team’s consideration: R4 – Please consider altering the wording of the final sentence of R4 to “The evaluation shall consider, at a minimum, the following:”. This allows additional flexibility for entities with existing physical security assessment programs to continue to include those extra elements within their plans. R5 – For the timeframe dependency please consider altering the dependent requirement to R4 instead of R2. Within the rationale section the drafting team concedes that R4 must be completed prior to commencing R5 and the drafting team also states that R4 does not state when the evaluation must occur, only that it must occur in time to meet R5. AET respectfully suggests

that a linear progression be established just as in R1, R2, and R3. This would require a timeline be added to R4 for the completion of the physical security risk assessment (AET suggests 120 calendar days from the completion of R2). AET also respectfully suggests that R5 then be made dependent on the completion of R4 (AET suggest 120 calendar days from the completion of R4). R6 – Please consider the removal of the required certifications in R6.1.1. The FERC order specifies that the risk assessment be reviewed by "[…] or another entity with appropriate expertise" and does not specify any particular qualifications. In addition, no other CIP standard calls for specific certifications or qualifications. Neither engineering focused requirements (e.g. CIP-002) or cyber security focused requirements (e.g. CIP-003, 005, 007) specify that those requirements be reviewed or implemented by designated engineers or certified security practitioners (e.g. CISSP). The due diligence required of the entity will determine the level of rigor that that entity is comfortable with defending and should not be included in the standard.
No
Individual
Richard Vine
California ISO
Agree
ISO/RTO Standards Review Committee
Individual
Mauricio Guardado
Los Angeles Department of Water and Power (LADWP)
Yes
LADWP requests the Drafting Team to make the following changes: - For Secion 4, you may want to add Transmission Planner and Planning Coordinator to the applicability. These functions may have responsibility on at least R1 and R2. - Secion 4.1.1.1 – Add "(AC or DC)" as follows: "Transmission Facilities operated at 500 kV (AC or DC) or higher….."
No
LADWP requests the Drafting Team to make the following changes: - For R1, additional time is needed to make sure studies are fully completed and reviewed by TO and its applicable governing authorities. Add ", which is due 30 calendar days after the effective date of the standard" to R1 as follows: "R1. Each Transmission Owner shall perform an initial risk assessment, which is due 30 calendar days after the effective date of the standard and subsequent risk assessments of its Transmission stations and Transmission substations (existing and……" - For R1, change "24 months" to " 30 months" to align the assessment with subsequent risk assessments. - For R2.1, The term "unaffiliated" needs to be defined in the standard to avoid any misinterpretation. - For R2.2, change the "90 calendar days" to "120 calendar days" to allow sufficient time to resolve differences if Planning Coordinator, Transmission Planner or Reliability Coordinator are addressing other deadlines.

No
LADWP requests the Drafting Team to make the following changes: - For R5, replace the word “implement” with “complete” to avoid confusion as to whether the plan needs to be implemented within the timeline provided - For R5.1, the word “Resiliency” needs to be defined in the standard to avoid any misinterpretation. Resiliency means different things to different people - For R5.1, add the language “, mitigate the impacts of,” to the requirement as follows: “5.1. Resiliency or security measures designed to deter, detect, delay, assess, communicate, mitigate the impacts of, and respond…..” - For R5.4, change the requirement language to read as follows: “5.4. Provisions to evaluate evolving physical threats to the Transmission station(s), Transmission substation(s), or primary control center(s), and their corresponding security counter measures. “ This sub-requirement should allow for the TO to revise its already-reviewed security plan within the 30-month cycle without necessarily having to make arrangements for a third party review of the revised plan (although it may do so if TO so desires) and without creating an additional 30-month cycle review that the normal course – this is a matter of efficiency and due diligence to address evolving threats - For 6.1, as previously mentioned, the word “unaffiliated” needs to be defined in the standard to avoid any misinterpretation. - For 6.1.3, change the requirement as follows: “6.1.3. A governmental agency with physical security expertise, which could be a City Department in which the utility resides that requires a review to be performed.” This clarification allows for additional flexibility of independent governmental agencies reviews. - For 6.1.4, change the requirement as follows: “6.1.4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise, such as the local police department in which the utility resides that requires a review to be performed.” This clarification allows for additional flexibility of independent entities or organizations reviews - For R6, add 6.1.5 with the following language: “6.1.5. A peer utility review group with demonstrated law enforcement, government, or military physical security expertise This clarification allows for additional flexibility of other Planning Coordinator, Transmission Planner or Reliability Coordinator review the work of their peers. In the alternative, expand to include Planning Coordinator, Transmission Planner or Reliability Coordinator with law enforcement, government, or military physical security expertise. - For 6.2, change the “90 calendar days” to “120 calendar days” to provide sufficient time to determine reasonable and sound recommendations. - For 6.3, chance the “90 calendar days” to “120 calendar days” to provide sufficient time to address any modifications recommended.
No
Individual
Laurie Williams
PNM Resources
EEI
No

R2.1 puts an unreasonable burden on registered PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO PNM can't force another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Group
Associated Electric Cooperative, Inc.- JRO00088
David Dockery
Agree
NRECA
Individual
Richard Vine
California ISO
Yes
Yes
We agree with the approach identified in R1 through R3, however we have the following comments regarding the SCOPE of the verification review required by R2.2: • The scope of the 3rd party verification is not well defined. What is the expectation and scope of the verification review? What level of quality is expected/required? Is the Transmission Owner responsible for scoping the verification process to ensure the review meets the required level of review? • Very little guidance is provided on the scope of the review. The scope of the review and verification work would need to be well understood before taking this verification work on. Is a technical analysis required as part of the review and verification process on the part of the 3rd party verifying the Transmission Owner's risk assessment and list of critical facilities, or is it simply to review the risk assessment and list of critical facilities that the Transmission Owner has provided to the 3rd party reviewer, based on their current knowledge of the transmission system from performing prior transmission planning studies? Will NERC be providing additional guidance regarding the scope of work required for verification by a 3rd party?
Yes
No
Group

Cooper Compliance Corp
Mary Jo Cooper
Yes
We support the applicability proposed by CIP-014-1.
No
We do not support the Standard as written today. We agree with the scope and content of the SAR. However, we are concerned with Requirement 6. Requirement 6 requires entities to seek out third parties to review their new physical security protection plans. We don't believe that entities should be obligated to seek assistance from third party individuals. This includes consultants or another unassociated entity. The purpose of the regions, NERC, and FERC are to provide a review of an entities compliance to Standards through the audit and self-certification process. No other Reliability Standards require an entity to use third parties to determine compliance or sufficiency of compliance documentation. We believe that this obligation may place some entities in difficult financial situation and could have a negative impacts in assuring that proper third party entities are being used. Should FERC, NERC, or WECC determine that entities are not following the spirit of the Standard than they may request a modification in a future Standard revision. We will support this Standard if Requirement 6 is removed.
No
We do not support the Standard for the same reason above. We do not support a third party review requirement other than that of the existing Standards. That is a review by FERC, NERC or the appropriate region.
Yes
We would like to address proposed comments by APPA that additional Standards are added to address confidentiality. We do not agree with APPA's position. The functional model requires registered functions to work together to secure reliability. Already, as a result of CIP Standards, vital communications between the Distribution Providers/Load Serving Entities and the Balancing Authorities and/or Transmission Operators have been compromised. Often, The Balancing Authorities and Transmission Operators are in fear of sharing important information with the Distribution Providers and/or Load Serving Entities because they feel they could be subject to a CIP violation. In some cases the Distribution Providers and Transmission Operators even share facilities. Having a requirement that prevents sharing vital information on physical security would simply not work and therefore we do not support APPA's comments.
Individual
Michael Mertz
PNM Resources
Yes
Support the comments submitted by EEI.

No
R2.1 could place an unreasonable burden on entities registered as PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO an entity cannot compel another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Yes
Support the comments submitted by EEI
Yes
Support the comments submitted by EEI
Individual
Jeffrey Fuller
Dayton Power & Light
Agree
Dayton Power & Light

Comments Received from Herb Schrayshuen

Question 1 – Response: No

Comments: The applicability of the standard is to Transmission Owners and Transmission Operators. Generating plants sites where the facilities production capability exceeds 1000 MW or other suitably larger amount should be included.

Question 2 – Response: No

Comments: In Requirement R1 the use of the term ‘transmission analysis’ and ‘transmission analyses’ in order to identify which substations should have a security plan is vague The TPL standards extreme cases should be used to clearly describe the specific required elements of the analysis. Failure to specify how the analysis is to be done will lead to inconsistencies in the analysis and thereby difficulty for audits of the standard.

In Requirement R2 the use of the word ‘unaffiliated’ introduces ambiguity. There needs to be an understanding (through the standard but if not feasible through RSAW or other tool-e.g. guideline) what “unaffiliated” means.

The term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities.

Question 4 – Response: Yes

Comments: The Implementation Plan can be read that it obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. The implementation plan should be adjusted.

The following is a suggestion to facilitate reading of the standard and stay whitn defined terms without introfucing new terms which are undefined: For all requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary.

While the requirement for unaffiliated third party verification of the physical security plan is something required by the FERC in its order, the mandate is misguided and will lead to security breaches while at the same time adding no incremental value to the physical security plan. The utility, which owns the assets, is already highly incentivized to put together a good security plan to avoid loss of its facilities to terrorism without third party verification. The utility may decide to use security consultants to help develop the plan if it involves new, state of the art physical security topics outside the utilities experience base. On balance the third party verification requirement outlined in R6 regarding the physical security plan is unneeded.

Additional comment received from Marcus Pelt, Southern Company

"The wording of Requirement R2.s, as it stands currently, could be interpreted to place requirements on the unaffiliated third party verifier when the responsible entity is actually the Transmission Owner. Southern recommends that R2.2 be reworded as follows to address this concern:

Proposed R2.2
2.2 The responsible Transmission Owner shall ensure the unaffiliated third party verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment. The unaffiliated third party verification may, but is not required to, include recommended additions or deletions of Transmission station(s) or Transmission substation(s)."

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project 2014-04 Physical Security

The Project 2014-04 Physical Security Standard Drafting Team (SDT) thanks all commenters who submitted comments on the CIP-014-1 standard. The standard was posted for a 15-day formal comment period from April 10-24, 2014. Stakeholders were asked to provide feedback on the standard and associated documents through a special electronic comment form. There were 136 sets of responses, including comments from approximately 240 different people from approximately 165 companies representing all 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the project page.

Summary Consideration:

The SDT has reviewed all comments and made the following non-substantive changes to the standard to incorporate stakeholder recommendations:

- Part 4.1.1 is modified:

  4.1.1 Transmission Owner that owns ~~any of the following~~ **a Transmission station or Transmission substation that meets any of the following criteria**:

- The applicability exemption contained Section 4 is modified:

  Exemption: Facilities **in a "protected area," as defined in 10 C.F.R. § 73.2,** within the scope of a security plan approved **or accepted** by the Nuclear Regulatory Commission **are not subject to this Standard;** or**, Facilities within the scope of a security plan approved by** the Canadian Nuclear Safety Commission are not subject to this Standard.

- Requirement R1 is modified:

  R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify ~~any~~ **the** Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

- Measure M1 is modified:

  M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission

substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. **Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.**

- Requirement R2 Part 2.2 is modified:

2.2 The unaffiliated ~~verifying entity~~ **third party verification** shall ~~either~~ verify the Transmission Owner's risk assessment performed under Requirement R1**,** ~~or recommend~~ **which may include recommendations** for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

- Requirement R2 Part 2.4 is modified:

2.4 Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~ **made available to** the unaffiliated **third party verifier** ~~verifying entity~~ **and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.**

- Measure M2 is modified:

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. **Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.**

- Requirement R3 is modified:

R3. For a primary control center(s) **of a Transmission station or Transmission substation** identified ~~by a transmission owner~~ according to Requirement R1**, Part 1.2 that a) operationally controls an identified Transmission Station or Transmission substation** ~~and~~ verified according to Requirement R2, **and b)** ~~that~~ is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

- Measure M3 is modified:

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic **notifications or** communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

- Requirement R4 is modified:

R4. Each Transmission Owner that ~~owns or operates~~ **identified** a Transmission station, Transmission substation, or **a** primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

- Requirement R4 Part 4.2 is modified:

4.2 Prior history ~~or~~ **of** attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

- Requirement R4 Part 4.3 is modified:

4.3 Intelligence or threat warnings **received** from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

- Requirement R5 is modified:

R5. Each Transmission Owner that ~~owns or has operational control of~~ **identified** a Transmission station, Transmission substation, or primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). **The physical security plan(s) shall be developed** within 120 calendar days following the completion of Requirement R2 **and executed according to the timeline specified in the physical security plan(s)**. The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

- Requirement R5 Part 5.1 is modified:

5.1 Resiliency or security measures designed **collectively** to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results~~ of **identified during** the evaluation conducted in Requirement R4.

- Requirement R5 Part 5.3 is modified:

5.3 A timeline for ~~implementing~~ **executing** the physical security enhancements and modifications specified in the physical security plan.

- Measure M5 is modified:

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating ~~implementation~~ **execution** of the physical security plan **according to the timeline specified in the physical security plan.**

- Requirement R6 is modified:

R6. Each Transmission Owner that ~~owns or operates~~ **identified** a Transmission station, Transmission substation, or primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

- Requirement R6 Part 6.1 is modified:

6.1 Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- ~~6.1.1~~ An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- ~~6.1.2~~ An entity or organization approved by the ERO.
- ~~6.1.3~~ A governmental agency with physical security expertise.

- ~~6.1.4~~ An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

- Requirement R6 Part6.3 is modified:

  6.3 If the unaffiliated **third party** ~~reviewing entity~~ **reviewer** recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Requirement R6 Part6.4 is modified:

  6.4 Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~ **made available to** the unaffiliated reviewing entity **and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure**.

- Measure M6 is modified:

  M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. **Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.**

A summary response to each comment follows each question. Please note that because common issues were grouped together in the summaries, an individual's comment may have been addressed in the summary for a question that is different from the question in which they submitted the comment; the SDT encourages reviewers to read all summary responses.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process! If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf

Index to Questions, Comments, and Responses

1. Applicability: The applicability of proposed CIP-014-1 starts with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a "medium impact" rating. The drafting team did not modify these criteria in their use under CIP-014-1, as they have been previously approved by stakeholders, NERC, and FERC. The SDT sought to ensure that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1. The team determined that slightly modified criteria could possibly result in confusion in application. The drafting team considered several other alternatives to refine the scoping in the applicability section, such as a particular kV threshold in addition to the other criteria; however, after significant discussion, the team found no technical or reliability basis for providing such limitiation. Importantly, by virtue of application of Requirement R1, the scope of the standard only applies to Transmission Owners that have Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers. Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In those cases, the entity only performs Requirements R1 through R2. When that results in a null set, Requirement R1 additionally provides that subsequent risk assessments may occur less frequently. Similarly, while Transmission Operators are also listed in the applicability section, by virtue of application of the requirements, only certain Transmission Operators that are notified under the standard's Requirement R3 have obligations under the standard. Do you agree with the applicability section? If not, please provide specific recommendations, ensuring to articulate how your suggested approach would not limit the applicability in such a manner as to inadvertently miss a facility that should be covered under the standard as specified in the FERC order on physical security. 27

2. Requirements R1 through R3: The first three requirements of CIP-014-1 require Transmission Owners to: (1) perform risk assessments to identify through transmission planning analysis those Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers, that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; (2) arrange for a third party verification (as directed in the order) of the identifications; and (3) notify certain Transmission Operators of identified primary control centers that operationally control the identified and verified Transmission stations and Transmission substations. The requirements provide the periodicity for satisfying these obligations. Only an

entity that owns or operates one or more of the identified facilities has further obligations in Requirements R4 through R6. If an entity identifies a null set after applying Requirements R1 through R2, the rest of the standard does not apply. Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security. 60

3. Requirements R4 through R6: The final three requirements of CIP-014-1 require (1) the evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified and verified according to the earlier requirements, (2) the development and implementation of a security plan(s) designed in response to the evaluation, and (3) a third party review of the evaluation and security plan(s) (as directed in the order). Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security. 111

4. Do you have input on other areas of the standard or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions. Please limit your response to 300 words or less. 152

The Industry Segments are:

1 — Transmission Owners
2 — RTOs, ISOs
3 — Load-serving Entities
4 — Transmission-dependent Utilities
5 — Electric Generators
6 — Electricity Brokers, Aggregators, and Marketers
7 — Large Electricity End Users
8 — Small Electricity End Users
9 — Federal, State, Provincial Regulatory or other Government Entities
10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Ben Engelby	ACES Standards Collaborators	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	John Shaver	Arizona Electric Power Cooperative/Southwest Transmission Cooperative, Inc.	WECC	1, 4, 5
2.	Shari Heino	Brazos Electric Power Cooperative, Inc.	ERCOT	1, 5
3.	Kevin Lyons	Central Iowa Power Cooperative	MRO	
4.	Amber Skillern	East Kentucky Power Cooperative	SERC	1, 3, 5
5.	Michael Brytowski	Great River Energy	MRO	1, 3, 5, 6
6.	Chip Koloini	Golden Spread Electric Cooperative, Inc.	SPP	5
7.	Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	RFC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

8.	Scott Brame	North Carolina Electric Membership Corporation	SERC	1, 3, 4, 5
9.	Mark Ringhausen	Old Dominion Electric Cooperative	SERC	3, 4
10.	Bill Hutchison	Southern Illinois Power Cooperative	SERC	1
11.	Dave Viar	Southern Maryland Electric Cooperative	RFC	3
12.	Ellen Watkins	Sunflower Electric Power Corporation	SPP	1
13.	Susan Sosbe	Wabash Valley Power Association	SERC	3

2.	Group	Paul Haase	APPA	X				X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Michael Shaw	LCAR	ERCOT	6
2.	Dixie Wells	LCRA	ERCOT	5
3.	Martyn Turner	LCRA	ERCOT	1

3.	Group	David Dockery	Associated Electric Cooperative, Inc.-JRO00088	X		X		X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3
3.	M & A Electric Power Cooperative		SERC	1, 3
4.	Northeast Missouri Electric Power Cooperative		SERC	1, 3
5.	N.W. Electric Power Cooperative, Inc.		SERC	1, 3
6.	Sho-Me Power Electric Cooperative		SERC	1, 3

4.	Group	Bob Case - NERC Compliance Manager , Bob.Case@blackhillscorp.com	Black Hills Corporation Entities	X		X	X	X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	NCR05030	Black Hills Power	WECC	1, 3, 4
2.	NCR05031	Black Hills Wyoming	WECC	5, 6
3.	NCR00089	Black Hills Colorado Electric	WECC	1, 3, 4
4.	NCR11186	Black Hills Colorado IPP	WECC	5, 6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5.	Group	Andrea Jessup	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Jeff Millennor	Physical Security	WECC	1
2.	Richard Becker	Substation Engineering	WECC	1
3.	Jim Burns	Technical Operations	WECC	1
4.	Kyle Kohne	Transmission Planning	WECC	1

6.	Group	Raymond G. Fugere	California Public Utilities Commission: Safety and Enforcenment Division									X	

	Additional Member	Additional Organization	Region	Segment Selection
1.	Benjamin Brinkman	California Public Utilities Commission: Safety and Enforcenment Division	WECC	9

7.	Group	Peter Yost	Con Edison and Orange & Rockland	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Edward Bedder	ORU	NPCC	1, 3

8.	Group	Mary Jo Cooper	Cooper Compliance Corp	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Draeger	Alameda Municipal Power		3
2.	Fred Fletcher	Burbank Water and Power		3
3.	Blain Ladd	California Pacific Electric Co.		3
4.	Mel Grandi	City of Ukiah		3
5.	Angela Kimmey	Pasadena Water and Power		1, 3
6.	Ken Dize	Salmon River Electric Coop		3

9.	Group	Connie Lowe	Dominion	X		X		X	X	X			

	Additional Member	Additional Organization	Region	Segment Selection
1.	Randi Heise	NERC Compliance Policy	MRO	5
2.	Mike Garton	NERC Compliance Policy	NPCC	5, 6

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

3.	Louis Slade	NERC Compliance Policy	RFC	
4.	John Loftis	Electric Transmission Compliance	SERC	1, 3, 5, 6
5.	Candace Marshall	Electric Transmission Compliance	SERC	1, 3, 5, 6
6.	Larry Nash	Electric Transmission Compliance	SERC	1, 3, 5, 6

10.	Group	Michael Lowman	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils		RFC	1
2.	Lee Schuster		FRCC	3
3.	Dale Goodwine		SERC	5
4.	Greg Cecil		RFC	6

11.	Group	Joe Tarantino	ERTF	X				X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Martyn Turner	LCRA	ERCOT	1
2.	Dixie	Wells	ERCOT	5

12.	Group	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Bill Smith	FE	RFC	1
2.	Cindy Stewart	FE	RFC	3
3.	Doug Hohlbaugh	FE	RFC	4
4.	Ken Dresner	FE	RFC	5
5.	Kevin Querry	FE	RFC	6

13.	Group	Frank Gaffney	Florida Municipal Power Agency	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tim Beyrle	City of New Smyrna Beach	FRCC	4
2.	Jim Howard	Lakeland Electric	FRCC	3
3.	Greg Woessner	Kissimmee Utility Authority	FRCC	3
4.	Lynne Mila	City of Clewiston	FRCC	3
5.	Cairo Vanegas	Fort Pierce Utility Authority	FRCC	4

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
6.	Randy Hahn	Ocala Utility Services	FRCC 3										
7.	Stanley Rzad	Keys Energy Services	FRCC 1										
8.	Don Cuevas	Beaches Energy Services	FRCC 1										
9.	Mark Schultz	City of Green Cove Springs	FRCC 3										
14.	Group	Greg Campoli	ISO/RTO Standards Review Committee		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ali Miremadi	CAISO	WECC	2
2.	Cheryl Moseley	ERCOT	ERCOT	2
3.	Ben Li	IESO	NPCC	2
4.	Matthew Goldberg	ISONE	NPCC	2
5.	Terry Bilke	MISO	RFC	2
6.	Stephanie Monzon	PJM	RFC	2
7.	Charles Yeung	SPP	SPP	2

15.	Group	Tom McElhinney	JEA	X		X		X					

	Additional Member	Additional Organization	Region	Segment Selection
1.	Ted Hobson		FRCC	1
2.	Garry Baker		FRCC	3
3.	John Babik		FRCC	5

16.	Group	Michael Jones	National Grid	X		X							

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brian Shanahan	National Grid	NPCC	3

17.	Group	Steve Hill	NCPA Compliance Management Operating Committee				X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Tracy Bibb	NCPA	WECC	4
2.	Scott Tomashefsky	NCPA	WECC	NA
3.	Hari Modi	NCPA	WECC	5

18.	Group	Brent Ingebrigtson	PPL NERC Registered Affiliates	X		X		X	X				

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Charlie Freibert	Louisville Gas and Electric Company and Kentucky Utilities Company	SERC	3
2.	Brenda Truhe	PPL Electric Utilties Corporation	RFC	1
3.	Annette Bannon	PPL Generation, LLC	RFC	5
4.		PPL Susquehana, LLC	RFC	5
5.		PPL Montana, LLC	WECC	5
6.	Elizabeth Davis	PPL EnergyPlus, LLC	MRO	6
7.			NPCC	6
8.			RFC	6
9.			SERC	6
10.			SPP	6
11.			WECC	6

19.	Group	Paul Haase	Seattle City Light	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Pawel Krupa	Seattle City Light	WECC	1
2.	Dana Wheelock	Seattle City Light	WECC	3
3.	Hao Li	Seattle City Light	WECC	4
4.	Mike Haynes	Seattle City Light	WECC	5
5.	Dennis Sismaet	Seattle City Light	WECC	6

20.	Group	Cynthia Hill-Watson	SERC CIPC	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Cynthia Hill-Watson	TVA	SERC	1, 3, 5, 6
2.	Jack Paul	TVA	SERC	1, 3, 5, 6
3.	Tony Hall	LGE-KU	SERC	1, 3, 5, 6
4.	Neil Phinney	GSOC	SERC	3, 4
5.	Mike Stanley	MEAG	SERC	1, 3, 5

21.	Group	Robert Rhodes	SPP Standards Review Group	X	X	X		X	X				

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

	Additional Member	Additional Organization	Region	Segment Selection
1.	Mo Awad	Westar Energy	SPP	1, 3, 5, 6
2.	Sandie Bayless	Westar Energy	SPP	1, 3, 5, 6
3.	Derek Brown	Westar Energy	SPP	1, 3, 5, 6
4.	Phil Clark	Grand River Dam Authority	SPP	1
5.	Louis Guidry	Cleco Power	SPP	1, 3, 5, 6
6.	Shannon Mickens	Southwest Power Pool	SPP	2
7.	James Nail	City of Independence, MO	SPP	3
8.	Jerald Nottnagel	Oklahoma Gas & Electric	SPP	1, 3, 5
9.	Terri Pyle	Oklahoma Gas & Electric	SPP	1, 3, 5
10.	Valerie Sesler	Westar Energy	SPP	1, 3, 5, 6
11.	Megan Wagner	Westar Energy	SPP	1, 3, 5, 6
12.	Ellen Watkins	Sunflower Electric Power Corporation	SPP	1

22.	Group	Ronald L Donahey	Tampa Electric Company	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Sara E Young	Tampa Electric Company	FRCC	1
2.	James Rocha	Tampa Electric Company	FRCC	5
3.	Benjamin Smith	Tampa Electric Company	FRCC	6
4.	Ronald L Donahey	Tampa Electric Company	FRCC	3

23.	Group	Brian Millard	Tennessee Valley Authority	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	DeWayne Scott		SERC	1
2.	Ian Grant		SERC	3
3.	David Thompson		SERC	5
4.	Marjorie Parsons		SERC	6

24.	Group	Lloyd A. Linke	Western Area Power Administration	X					X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Western Area Power Administraton	Upper Great Plains Region	MRO	1, 6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
2. Western Area Power Administraton			Rocky Mountain Region WECC 1, 6										
3. Western Area Power Administraton			Desert Southwest Region WECC 1, 6										
4. Western Area Power Administraton			Colorado River Storage Project WECC 6										
5. Western Area Power Administraton			Sierra Nevada Region WECC 1, 6										
25.	Individual	David Jendras	Ameren	X		X		X	X				
26.	Individual	Thomas Foltz	American Electric Power	X		X		X	X				
27.	Individual	Allen Mosher	American Public Power Association (APPA)	X		X	X	X	X				
28.	Individual	Andrew Z. Pusztai	American Transmission Company, LLC	X									
29.	Individual	Joe Tarantino	APPA	X		X	X	X	X				
30.	Individual	Janet Smith	Arizona Public Service Company	X		X		X	X				
31.	Individual	Glen Sutton	ATCO Electric	X									
32.	Individual	David Rudolph	Basin Electric Power Cooperative (BEPC)	X		X		X					
33.	Individual	Erika Doot	Bureau of Reclamation	X				X					
34.	Individual	Richard Vine	California ISO		X								
35.	Individual	Richard Vine	California ISO		X								
36.	Individual	Raymond Fugere	California Public Utilities Commission: Safety and Enforcenment Division									X	
37.	Individual	Frank Pace	Central Hudson Gas & Electric Corporation	X									
38.	Individual	Kevin Lyons	Central Iowa Power Cooperative	X		X							
39.	Individual	Chad Bowman	CHPD	X									
40.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
41.	Individual	Ronnie C. Hoeinghaus	City of Garland	X		X							
42.	Individual	Bill fowler	City of Tallahassee			X							
43.	Individual	Scott Langston	City of Tallahassee	XX									
44.	Individual	John Allen	City Utilities of Springfield, Missouri										
45.	Individual	David Grubbs	Ciy of Garland	X		X		X	X				
46.	Individual	Jack Stamper	Clark Public Utilities	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
47.	Individual	Shannon Fair	Colorado Springs Utilities	X		X		X	X				
48.	Individual	Robert Trowbridge	Consumers Energy Company			X		X					
49.	Individual	David Kiguel	David Kiguel								X		
50.	Individual	David Dworzak	Edison Electric Institute	X									
51.	Individual	Earl F. Cass	EF Cass Consulting Inc.								X		
52.	Individual	Mike Kidwell	Empire District Electric Company					X					
53.	Individual	Steve Hamburg	Encari	X									
54.	Individual	Dean Ahlsten	Eugene Water & Electric Board				X						
55.	Individual	Chris Scanlon	Exelon	X		X	X	X	X				
56.	Individual	Linda Jacobson-Quinn	FEUS			X							
57.	Individual	Russ Schneider	Flathead Electric Cooperative, Inc.			X	X						
58.	Individual	Dennis Minton	Florida Keys Electric Cooperative	X									
59.	Individual	Curtis Klashinsky	FortisBC	X									
60.	Individual	William R. Harris	Foundation for Resilient Societies								X		
61.	Individual	Guy Andrews	Georgia System Operations Corporation			X	X						
62.	Individual	David Revill	Georgia Transmission Corporation	X									
63.	Individual	Ladeene Freimuth	GridWise Alliance	X	X	X	X	X					
64.	Individual	Ayesha Sabouba	Hydro One	X		X							
65.	Individual	Chantal Mazza	Hydro QuÃ©bec TransÃ‰nergie	X									
66.	Individual	Mike Marshall	Idaho Power Co.	X									
67.	Individual	Bob Thomas and Kevin Wagner	Illinois Municipal Electric Agency				X						
68.	Individual	Mark Wilson	Independent Electricity System Operator		X								
69.	Individual	John Falsey	Invenergy LLC					X					
70.	Individual	Michael P Moltane	ITC	X									
71.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
72.	Individual	Larry Watt	Lakeland Electric	X									
73.	Individual	Kayleigh Wilkerson	Lincoln Electric System	X		X		X	X				
74.	Individual	Mauricio Guardado	Los Angeles Department of Water and Power (LADWP)	X		X		X	X				
75.	Individual	Dixie Wells	Lower Colorado River Authority					X					
76.	Individual	Donald E Nelson	MA Dept. of Public Utilities									X	
77.	Individual	Shirley Mayadewi	Manitoba Hydro	X		X		X	X				
78.	Individual	David Gordon	Massachusetts Municipal Wholesale Electric Company					X					
79.	Individual	Gary Kruempel	MidAmerican Energy Holding Company	X		X		X	X				
80.	Individual	Randi Nyholm	Minnesota Power	X									
81.	Individual	Dan Inman	Minnkota Power Cooperative	X									
82.	Individual	David Francis	MISO		X								
83.	Individual	Nick Braden	Modesto Irrigation District			X	X		X				
84.	Individual	Barry Lawson	National Rural Electric Cooperative Association (NRECA)				X						
85.	Individual	Tony Eddleman	Nebraska Public Power District	X		X		X					
86.	Individual	Alan MacNaughton	New Brunswick Power Corporation	X									
87.	Individual	Wayne Sipperly	New York Power Authority	X		X		X	X				
88.	Individual	Bruce Metruck	New York Power Authority	X									
89.	Individual	Joe O'Brien	NIPSCO	X		X		X	X				
90.	Individual	Terry Volkmann	None	X									
91.	Individual	Guy Zito	Northeast Power Coordinating Council										X
92.	Individual	William Temple	Northeast Utilities	X									
93.	Individual	John Canavan	NorthWestern Energy	X									
94.	Individual	Alan Johnson	NRG Energy, Inc.			X	X	X	X				
95.	Individual	Venona Greaff	Occidental Chemical Corporation							X			

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
96.	Individual	Bernard Johnson	Oglethorpe Power Corporation					X	X				
97.	Individual	Donna Johnson	Oglethorpe Power Corporation						X				
98.	Individual	Mahmood Safi	Omaha Public Power District	X		X		X	X				
99.	Individual	David Ramkalawan	OPG					X					
100.	Individual	John Hagen	Pacific Gas and Electric Company	X		X		X					
101.	Individual	Jared Shakespeare	Peak Reliability	X									
102.	Individual	David Thorne	Pepco Holdings Inc.	X		X							
103.	Individual	Laurie Williams	PNM Resources	X		X							
104.	Individual	Michael Mertz	PNM Resources			X							
105.	Individual	Debra Horvath	Portland General Electric	X		X		X	X				
106.	Individual	Steven Wickel	Public Utility District No. 1 of Chelan County	X		X		X	X			X	
107.	Individual	John Yale	Public Utility District No. 1 of Chelan County	X		X		X	X			X	
108.	Individual	Hugh Owen	Public Utility District No. 1 of Chelan County						X				
109.	Individual	Michiko Sell	Public Utility District No. 2 of Grant County, WA	X		X		X	X			X	
110.	Individual	Kenn Backholm	Public Utility District No.1 of Snohomish County	X		X	X	X	X			X	
111.	Individual	Russell Noble	Public Utitliy District No. 1 of Cowlitz County, WA			X	X	X					
112.	Individual	Greg Froehling	Rayburn Country Electric Cooperative			X							
113.	Individual	Anthony Jablonski	ReliabilityFirst										X
114.	Individual	Joshua Andersen	Salt River Project	X		X		X	X				
115.	Individual	Jennifer Wright	San Diego Gas & Electric	X		X		X					
116.	Individual	Debra Warner	self								X		
117.	Individual	Michael Haff	Seminole Electric Cooperative, Inc.	X		X	X	X	X				
118.	Individual	RoLynda Shumpert	South Carolina Electric and Gas	X		X		X	X				
119.	Individual	Patrick Farrell	Southern California Edison Company	X		X		X	X				

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
120.	Individual	Marcus Pelt	Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	X		X		X	X				
121.	Individual	Lynnae Wilson	Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	X		X		X	X				
122.	Individual	Bob Reynolsa	Southwest Power Pool Regional Entity										X
123.	Individual	David Godfrey	Texas Municipal Power Agency					X					
124.	Individual	Derrick Davis	Texas RE										X
125.	Individual	Ralph Meyer	The Empire District Electric Company	X									
126.	Individual	Kalem Long	The Empire District Electric Company			X							
127.	Individual	Eric Olson	Transmission Agency of Northern California	X									
128.	Individual	Sergio Banuelos	Tri-State Generation and Transmission Association, Inc.	X		X		X					
129.	Individual	Melissa Kurtz	US Army Corps of Engineers					X					
130.	Individual	Brian Evans-Mongeon	Utility Services				X						
131.	Individual	kim moulton	Vermont Transco LLC	X									
132.	Individual	William H. Chambliss, member Operating Committee	Virginia State Corporation Commission										
133.	Individual	Candace Morakinyo	We Energies			X	X	X	X				
134.	Individual	Megan Wagner	Westar Energy	X		X							
135.	Individual	Steve Rueckert	Western Electricity Coordinating Council										X
136.	Individual	Amy Casuscelli	Xcel Energy	X		X		X	X				

If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).

Organization	Agree	Supporting Comments of "Entity Name"
Central Iowa Power Cooperative	Agree	ACES
MA Dept. of Public Utilities	Agree	Agree with the comments made by NPCC.
Massachusetts Municipal Wholesale Electric Company	Agree	American Public Power Association
Transmission Agency of Northern California	Agree	American Public Power Association
Eugene Water & Electric Board	Agree	American Public Power Association (APPA)
City of Austin dba Austin Energy	Agree	American Public Power Association (APPA). In addition, Austin Energy states the following:The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this Standard may be subject to disclosure under state open records laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard designating the produced, gathered, used and maintained records related to compliance with

Organization	Agree	Supporting Comments of "Entity Name"
		this Standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure.
JEA	Agree	APPA
City of Tallahassee	Agree	APPA
City of Tallahassee	Agree	APPA
City Utilities of Springfield, Missouri	Agree	APPA
New York Power Authority	Agree	APPA
New York Power Authority	Agree	APPA
Public Utility District No. 1 of Chelan County	Agree	APPA and LPPC comments
FEUS	Agree	APPAWECC
NorthWestern Energy	Agree	Arizona Public Service, Bureau of Reclamation, Portland General Electric, WECC
California Public Utilities Commission: Safety and Enforcenment Division	Agree	California Public Utilities CommissionSafety and Enforcenment Division
CHPD	Agree	CHPD is supportive of the comments submitted by APPA
Texas Municipal Power Agency	Agree	City of Garland and American Public Power Assocation

Organization	Agree	Supporting Comments of "Entity Name"
We Energies	Agree	Edison Electric Institute (EEI)
Lakeland Electric	Agree	Florida Municipal Power Agency (FMPA)
Illinois Municipal Electric Agency	Agree	Florida Municipal Power AgencyAmerican Public Power Association
Oglethorpe Power Corporation	Agree	Georgia Transmission Corporation (GTC)National Rural Electric Cooperative Association (NRECA)
Oglethorpe Power Corporation	Agree	Georgia Transmission Corporation (GTC)National Rural Electric Cooperative Association (NRECA)
Occidental Chemical Corporation	Agree	Ingleside Cogeneration, LP
California ISO	Agree	ISO/RTO Standards Review Committee
Lower Colorado River Authority	Agree	Lower Colorado River Authority
Public Utility District No. 1 of Chelan County	Agree	LPPC and APPA
Public Utility District No. 1 of Chelan County	Agree	LPPC and APPA
Invenergy LLC	Agree	NPCC
Associated Electric Cooperative, Inc.- JRO00088	Agree	NRECA

Organization	Agree	Supporting Comments of "Entity Name"
Public Utility District No.1 of Snohomish County	Agree	Salt River Project ("SRP")
ERTF	Agree	The following comments are in agreement with LPPC and ERTF as well as comment from our own entity LCRA: o Use of "primary control center" is ambiguous (R1.2 and others); o Unaffiliated third party review needs to be longer than 90-days, suggestion to be 180-days (R2.2); o Issue with non-disclosure agreement vs. Public Power's obligation to disclose information (R2.4); o Expansion of the Security Plan third-party reviewer to include those functions that are identified in Requirement 2.1 (R6.1). o The standard does not address substations/stations that are owned by multiple Transmission Owners. LCRA TSC recommends adding language describing NERC's expectations associated with jointly-owned substations/stations or substation/stations with multiple asset owners.
APPA	Agree	The stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section: 7. Critical Facilities Information Records and related information concerning critical facilities, physical infrastructure,

Organization	Agree	Supporting Comments of "Entity Name"
		including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language (new subrequirements): R1 1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard. R3 3.4 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under Requirement R1 of this standard. R4 4.1 The Transmission Owner will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 conducted under this standard.
US Army Corps of Engineers	Agree	Western Area Power Administration

Organization	Agree	Supporting Comments of "Entity Name"
Public Utitliy District No. 1 of Cowlitz County, WA		American Public Power Association
APPA		American Public Power Association (APPA)
Colorado Springs Utilities		CSU agrees with APPA comments with exception to the confidentiality section, please see CSU's comments below.CONFIDENTIALITYPublicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background:7. Critical Facilities InformationRecords and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted

Organization	Agree	Supporting Comments of "Entity Name"
		under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS:R1.3 All records and information related to the risk assessments conducted of this standard are exempt from public disclosure.R3.2 All records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard are exempt from public disclosure. R4.4 All records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1 of this standard are exempt from public disclosure.Adding confidential in the standard would create undo compliance burden and auditing challenges.
PNM Resources		EEI
Modesto Irrigation District		Modesto Irrigation District supports the comments submitted by American Public Power Association/Large Public Power Council
Seminole Electric Cooperative, Inc.		National Rural Electric Cooperative Association (NRECA)
Public Utility District No. 2 of Grant County, WA		Public Utility District No. 2 of Grant County, WA

1. **Applicability: The applicability of proposed CIP-014-1 starts with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a "medium impact" rating. The drafting team did not modify these criteria in their use under CIP-014-1, as they have been previously approved by stakeholders, NERC, and FERC. The SDT sought to ensure that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1. The team determined that slightly modified criteria could possibly result in confusion in application. The drafting team considered several other alternatives to refine the scoping in the applicability section, such as a particular kV threshold in addition to the other criteria; however, after significant discussion, the team found no technical or reliability basis for providing such limitation. Importantly, by virtue of application of Requirement R1, the scope of the standard only applies to Transmission Owners that have Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers. Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. In those cases, the entity only performs Requirements R1 through R2. When that results in a null set, Requirement R1 additionally provides that subsequent risk assessments may occur less frequently. Similarly, while Transmission Operators are also listed in the applicability section, by virtue of application of the requirements, only certain Transmission Operators that are notified under the standard's Requirement R3 have obligations under the standard. Do you agree with the applicability section? If not, please provide specific recommendations, ensuring to articulate how your suggested approach would not limit the applicability in such a manner as to inadvertently miss a facility that should be covered under the standard as specified in the FERC order on physical security.**

Summary Consideration: The SDT thanks all commenters. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Part 4.1.1 was changed to clarify that applicable TO's are those that own transmission stations or transmission substations meeting the criteria in 4.1.1.1 through 4.1.1.4. The exemption for nuclear facilities was changed to provide more specific criteria in terms of the security plans under Nuclear Regulatory Commission or Canadian Nuclear Safety Commission jurisdiction. Several additions were made to the guidance section of the standard to address stakeholder concerns. A summary of comments and the SDT's response is provided**:**

- **Several commenters suggested adding verbiage to the applicability regarding the Transmission Operator to refer to Requirement R3.** The SDT considered this wording during its deliberations and determined it was not necessary as Requirement R3 is explicit in its applicability to only certain Transmission Operators. The SDT notes that, in general, Requirements are not included in the applicability Section of the standard.

- **One commenter suggested applying the standard to Reliability Coordinators (RC) and only the Transmission Operators the RCs deem critical.** The majority of stakeholders concur with the applicability as written. This suggested revision would be a major shift in philosophy and thus the SDT will not make the change.
- **Some commenters suggested that the Reliability Coordinator, Planning Coordinator and Transmission Planner should be added to the Applicability Section.** During the initial deliberations, the SDT considered requiring RCs, PCs and TPs to conduct the R2.2 verification but developed an alternative that was included in the original standard, given that it did not believe it was appropriate or necessary to require RCs, PCs or TPs to be required to conduct the R2.2 verification. R2.2 may be performed by a variety of entities or consultants. It is the responsibility of the Transmission Owner or Transmission Operator to ensure that the third party agreements are written with performance requirements to meet the time-line of R2.2.
- **Several stakeholders had comments about confidentiality, especially with respect to federal and state public disclosure laws applicable to registered entities, such as state regulatory agencies and municipal entities.** The SDT has drafted language in Requirement R2, Part 2.4, Requirement R6, Part 6.4 and Section 1.4 of the Compliance section of the standard to address confidentiality. Specifically, Compliance Section 1.4 states:

  Additional Compliance Information

  "Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities."

Requirement R2, Part 2.4 now provides:

> Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated verifying entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

Lastly, Requirement R6, Part 6.4 now provides:

> Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated reviewing entity and from any other form of public disclosure and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

Collectively, these provisions are designed to protect sensitive and confidential information from public disclosure consistent with the intent of paragraph 11 of the FERC order on physical security. Because the scope and intent of NERC standards is to set forth the requirements that owners, operators and users must follow to help protect the reliability of the Bulk-Power System,

the SDT concluded that it is beyond the scope of NERC Reliability Standards to specify whether certain information is exempt from U.S. or Canadian federal or state public disclosure laws. However, the SDT included language in Parts 2.4 and Parts 6.4 of the standard to clarify that entities shall have procedures to protect or exempt sensitive or confidential information developed under the standard from public disclosure. The SDT believes that responsible entities have existing mechanisms for safeguarding confidential or sensitive information used to comply with existing NERC Reliability Standards and also recognizes that there are other forums that can address the applicability of this information to public disclosure laws.

- **Several commenters had concerns with the term "collector bus" as used in the applicability.** The SDT notes that this language was copied directly from the CIP-002-5.1 standard. The SDT has also added language to the Guidelines and Technical Basis section to clarify the use of the term collector bus.
- **Several commenters suggested making revisions to the table in 4.1.1.2.** The SDT notes that this was copied directly from CIP-002-5.1. This language was used to mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1.
- **One commenter suggested revising the applicability to indicate that only a Transmission Owner "that owns any facilities identified in the following sections (4.1.1.1 through 4.1.1.4) will be required to perform the risk assessment and risk assessment validation as outlined in R1 and R2 of this standard."** The SDT notes that this is addressed in the Guidelines and Technical Basis section and that the requirements make this clear.
- **Several commenters requested additional guidance regarding "unaffiliated" third party reviewers.** The SDT has provided additional guidance in the Guidelines and Technical Basis section as well as revisions to Requirement R2, Part2.2 and the Rationale for R2.
- **Some commenters have concerns and recommended that the Applicability section reference the criteria of CIP-002-5.1 for a "medium impact rating" instead of re-stating it and questioned certain aspects of the applicability.** The SDT believes that the Standard and Guidelines and Technical Basis section clearly indicates that the risk assessment is to only identify a Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The SDT notes that this was copied directly from CIP-002-5.1. This language was used to mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1.
- **Some commenters disagree with the decision to limit applicability to only the primary control center.** The SDT believes that providing physical security for the primary control center and not back-up control centers is sufficient to protect the control of the critical Transmission stations and Transmission substations. Back-up control centers are not applicable, as they are already considered a form of resiliency and intentionally redundant.

- **Some commenters believed that the SDT did not go far enough in the applicability of facilities, in particular with respect to physical locations where critical cyber systems are housed and high impact control centers.** The SDT disagrees as the standard follows the FERC Order and employs a risk assessment designed to identify a Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Such a scope is different than the scope of other CIP standards to protect cyber assets.
- **Some commenters question why generation assets are exempt from analysis and verification required by Requirements R1 and R2.as they assert that some generation assets, if rendered inoperable, could result in widespread instability, uncontrolled separation, or Cascading.** The SDT considered whether to include Generator Operators and Generator Owners in the proposed Reliability Standard and decided not to include them as applicable entities. First, the FERC Order does not explicitly mention generation assets, and the order is reasonably understood to focus on the most critical Transmission Facilities. Second, the proposed Reliability Standard accounts for the loss of generation resources as explained in the Guidelines and Technical Basis section. A determination of whether a Transmission station or Transmission substation that meets CIP-002-5.1's medium impact criteria could, if rendered inoperable or damaged, result in widespread instability, uncontrolled separation, or Cascading within an Interconnection will consider the impact of the loss of generation at those Transmission stations or Transmission substations. Specifically, the transmission analysis or analyses conducted under Requirement R1 will take into account the impact of the loss of generation. As such it is not necessary to include Generator Operators and Generator Owners to ensure that the impact of loss of generation is considered.
- **One commenter disagreed with the SDT that many entities that are applicable to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.** The SDT members were selected based on their expertise. To more explicitly or in greater detail explain their statements related to the number of Transmission stations or Transmission substations that will be identified in R1 would likely disclose information that is confidential and contrary to national security. In the order, FERC states this opinion in paragraph 12 as well.
- **One stakeholder commented that the standard is too complicated of a draft standard for a 90 day consensus and that it should be simplified by altering the basic approach of the standard.** While the SDT appreciates suggestions on altering the basic approach, it believes it struck the right balance to be consistent with and responsive to the FERC Order and provide for an applicability that has been approved by stakeholders and regulators.
- **Some commenters had concerns regarding the language in the Exemption regarding nuclear facilities.** The SDT has added clarifying language to the exemption to address these concerns.
- **One commenter questioned why a Transmission Owner must go through requirements R1 and R2 before determining whether or not the remaining requirements apply.** TOs that meet the applicability criteria (Section 4) need to perform the risk assessment (R1) and have it verified (R2) regardless of their size. This will identify the critical stations. This concept is provided

in the first paragraph of the Guidelines and Technical Basis section of the standard: "Only those TOs with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6."

- **Many commenters requested additional guidance regarding Transmission Facility, Transmission station and Transmission substation**. The SDT has added clarifying language to the Guidelines and Technical Basis section of the standard.
- **Several commenters suggested that the SDT use the defined term "Control Center" in the standard.** The SDT deliberated this during the development of the standard but did not believe that it was clearly applicable to this standard because a Control Center includes the RC, BA and GOP. These entities are not applicable under this standard. The SDT has decided to retain the original language.
- **One commenter suggested adding the primary control center to the applicability section of the standard.** The SDT deliberated this in previous meetings but decided it was not appropriate. The SDT will retain the existing applicability as we believe that stakeholder consensus has been achieved.
- **Several commenters had concerns with the requirements language regarding the timing components.** The SDT has added language to the guidance to help clarify these issues. The SDT believes that the timelines are aggressive but achievable. Please see responses to specific timing requirements in other questions below.
- **One commenter suggested adding "AC and DC" to the applicability.** The SDT does not believe that this is necessary as the voltage levels shown imply this.

Organization	Yes or No	Question 1 Comment
Foundation for Resilient Societies	No	1. Reliability Coordinators (RCs) would be exempted under the draft standard. Not all Reliability Coordinators are Transmission Operators or Owners. Peak Reliability, Midcontinent ISO, and Southwest Power Pool would be exempted because they are not in the NERC Compliance Registry as Transmission Operators or Owners. (MISO is not a Reliability Coordinator under its MRO registration.) The following standards apply to Reliability Coordinators but not Transmission Operators and Owners: Standard EOP-006-2 - "System Restoration Coordination"; Standard EOP-002-3.1 - "Capacity and Energy Emergencies" (Applies to Balancing Authorities, Reliability Coordinators, and Load-Serving Entities); Standard IRO-009-1 - "Reliability Coordinator Actions to Operate Within IROLs"; Standard IRO-015-1 - "Notifications and Information Exchange

Organization	Yes or No	Question 1 Comment
		Between Reliability Coordinators." The Joint U.S.-Canada report on the 2003 Blackout concluded that insufficient wide-area control, such as that provided by Reliability Coordinators, was a contributing factor to the blackout. Yet the Standard Drafting Team has disregarded these findings in exempting Reliability Coordinators. It is a fallacy to believe that only entities with direct control of substations need protection from physical attack. If critical substations and their Reliability Coordinators are attacked in a coordinated manner, what entity will lead system restoration? It is essential that Reliability Coordinators are designated as responsible entities, both to protect their own facilities and to enable their authority to review the adequacy of physical security capabilities for operating utilities in their coordinating areas. Key findings of the joint U.S.-Canada Outage Task Force on the August 2003 blackout demonstrated the need for the Reliability Coordinators to actively supervise operating entities both to meet essential operating needs and to assure adequate regional visibility. See U.S.-Canada Power System Outage Task Force Report (April 2004). <http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>2. Balancing Authorities would be exempted under the standard. According to the NERC Compliance Registry, there are 19 Balancing Authorities that are not also Transmission Operators or Owners. The following standards apply to Balancing Authorities but not to Transmission Operators or Owners: Standard BAL-001-2 - "Real Power Balancing Control Performance"; Standard BAL-002-1 - "Disturbance Control Performance"; Standard BAL-003-1 - "Frequency Response and Frequency Bias Setting"; Standard BAL-004-0 - "Time Error Correction"; Standard EOP-002-3.1 - "Capacity and Energy Emergencies"; Standard IRO-006-5 - "Reliability Coordination - Transmission Loading Relief". If critical substations and their Balancing Authorities are attacked in a coordinated manner, what entity will balance demand and generation and manage the emergency, especially if the attack causes a regional load imbalance?3. Generator Operators would be exempted under the proposed standard. Generator Operators have vulnerable and hard-to-replace Generator Step Up

Organization	Yes or No	Question 1 Comment
		(GSU) Transformers, just as Transmission Operators have these transformers. Generation facilities could present contingencies in excess of spinning reserves, especially in congested areas with import of large megawatts of power over long transmission lines. Hence, Generator Operators should be included in mandatory physical security protection standards.4. The standard does not require modeled contingency planning for scenarios of physical attack. Contingency planning for physical attack should include megawatt capacity of all generators at single generation facility, not just failure of some individual units at the facility.5. Without explicit modeling for physical attack, some substations may fall through the cracks under "Aggregate Weighted Value" methodology in the standard. Physical attack of multiple transformers is different than the random failures planned for under the standard N-1 criterion. We have already seen attack on multiple transformers and their circuits at the Metcalf substation. The standard's criterion for violation of IROL limits would not be valid if the IROL limits assume random failures rather than coordinated physical attack.6. Some "High Impact" control centers would be exempt under the standard. Examples include the control centers for Peak Reliability, MISO, and SPP. In all, these control centers manage power for 141 million Americans. Control centers for Reliability Coordinators, Balancing Authorities, and Generator Operators are included in the "High Impact" Criteria for CIP-002-5.1 How can the standard drafting team take the CIP-002-5.1 criteria for substations but not control centers of Reliability Coordinators, Balancing Authorities, and Generator Operators? FERC Directive RD14-6-000 specifically requires protection of critical control centers in Footnote 6: "... the Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."7. While FERC Directive RD14-6-000 [146 FERC Â¶61,166] did not require specific security measures, it could have been reasonably expected that NERC would have developed specific measures to be applied on an as-needed basis. Nonetheless, the draft standard contains no specific requirements or even suggested guidelines for physical security measures. Such measures

Organization	Yes or No	Question 1 Comment
		might include: Opaque Fencing; Concrete Jersey Barriers; Motion Sensors; License Plate Scanners; Intentional Electromagnetic Interference (IEMI) Detectors; Gunfire Locators; Limiting of Close Public Access, Including Recreational Access; Armed Private Guards; Police Details; Deployment of National Guard Troops; Better Stocking of Spares-e.g., Transformer Bushings and Radiators; Equipment Monitoring and Redundant Telemetry to Control Centers. Instead, the standard relies upon self-devised security measures without prioritization or other guidance.8. The Metcalf incident unambiguously showed the value of equipment monitoring in mitigating physical attack on power transformers. Gunfire locators, had they been installed at Metcalf, could have alerted system operators to the attack in real-time, allowing prompt dispatch of law enforcement. Intentional Electromagnetic Interference (IEMI) Detectors could likewise provide real-time warning. If threat sensors with reliable and cyber-protected alerts are not part of a physical security system, it will be impossible to mobilize time-urgent countermeasures and impractical to take precautionary measures at other at-risk facilities vulnerable to coordinated attack.9. Intentional Electromagnetic Interference should be a physical threat included in the standard, because IEMI attack could occur in the physical proximity of facilities and could cause permanent physical damage in additional to temporary upset. IEMI detectors are a cost-effective measure as these devices cost approximately $15,000 per unit.10. The Metcalf Incident was both a physical attack and a cyber denial-of-service attack. The need for linkage between physical and cyber is explicitly called for in the RD14-6-000 Order of March 7, 2014, para 5, footnote 3. The implementation plan under this Order must require responsible entities to identify and protect cyber assets that link facilities and control centers that are otherwise identified as critical to the reliability of the BES. Communications and Network entities routinely provide hardened and alternate routing for military, other government and the Defense Industrial Base and their services should be an explicit requirement for Physical Security Standards that apply to any units and control centers that are identified

Organization	Yes or No	Question 1 Comment
		by Responsible Entities as critical to the Reliability of the BES.11. Review and certification of security plans, as proposed in the draft standard, does not necessarily provide a level of independence that would be prudent or credible to the public. Regional Entities or Reliability Coordinators for any facilities under their jurisdiction should be the primary authorities to review and approve security plans. Governmental authorities should have the ability to audit security plans.12. Improvements to the standard that we suggest would be marginal additions of facilities and their equipment and therefore would be cost-effective. We propose inclusion of primary and backup control centers for Peak Reliability, MISO, and SPP-an increase of 6 control centers as compared to approximately 200 already included Transmission Operator control centers. We propose inclusion of 19 additional Balancing Authorities as compared to 114 Balancing Authorities in total. There are only 50 non-nuclear generation facilities in the United States with nameplate capacity of 2 GW or more-this number is a rough approximation of the number of generation facilities that modeling might show to be capable of causing cascading outage if successfully attacked.13. RD14-6-000 directs NERC to submit for approval a physical security standard that would apply to the most critical facilities of the Bulk Electric System. The Standard Drafting Team has narrowly interpreted “critical facilities” to mean transmission facilities and directly linked control centers. We disagree with this narrow interpretation. Given the NERC interpretation and the 90 day deadline for standard development, NERC’s draft standard holds tightly to the most minimal facilities and therefore has significant gaps in protection as we describe in our foregoing comments. Some of these gaps, such as the exemption of Reliability Coordinators and Balancing Authorities, are so fundamental that they should be addressed immediately. For other gaps, we ask that NERC open a Standard Authorization Request (SAR) for a Phase Two physical security standard. This follow-on Phase Two standard should require modeling of BES operations sufficient to ensure identification of facilities that could cause cascading outage, single points of failure, data connectivity needs, and other processes and

Organization	Yes or No	Question 1 Comment
		technologies essential to grid protection-in short, a standard designated CIP-014 Version 2. An approved SAR for a Phase Two standard should be concurrent with NERC Board of Trustees approval of the current standard in development.
Florida Keys Electric Cooperative	No	o Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is FKEC's understanding that a "station" equates to a switchyard that does not include transformers; and a "substation" is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard. o Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
Ciy of Garland	No	Applicability:The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective:4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3.Please state clearly the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.
Black Hills Corporation Entities	No	Black Hills Corporation (referred to as BHC hereafter) believes that Section 4.1.1 has appropriate applicability specifics, but Section 4.1.2 only says "Transmission Operator", which initially implies a much greater scope. Request that similar to

Organization	Yes or No	Question 1 Comment
		Section 4.1.1 styling, Section 4.1.2 alternatively state “Transmission Operators notified by a Transmission Owner according to Requirement R3.”
Nebraska Public Power District	No	Due to the imposed time constraints and expedited development of this standard, sufficient time isn’t available to develop more realistic criteria for determining applicable substations creating unnecessary work and expense for transmission planners and reviewers.
Georgia System Operations Corporation	No	Georgia System Operations Corporation (GSOC) appreciates all the effort going into the draft of CIP-014-1 Physical Security Reliability Standard.GSOC supports the comments submitted by NRECA.
Georgia Transmission Corporation	No	Georgia Transmission Corporation (GTC) supports the efforts of the drafting team and believes that their efforts to create the CIP-014 Standard are moving in the right direction. GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.
OPG	No	In the applicability section of the proposed standard, does the exemption refer to the Nuclear Generation Facility or the Transmission facility to which the Nuclear Generation Facility is connected? In Canada the Canadian Nuclear Safety Commission has no jurisdiction over the Transmission Owner/Operator; therefore the intent of the standard has to be made clear on this point.
Modesto Irrigation District	No	MID agrees that maintaining selection criteria consistent with CIP-002-5 is a prudent approach. However, if a facility is worthy of protection against a cyber attack, why is that same facility not worthy of consideration and evaluation for a potential physical attack? Inclusion of 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' as an additional criteria is also prudent. These criteria focus on the immediate impact of the physical attack. What is missing is the longer term impact - if serious physical damage is

Organization	Yes or No	Question 1 Comment
		the result, can the damaged system perform adequately during subsequent peak loading periods?MID understands that these changes would extent the scope of the standards coverage beyond what was included in the FERC order. MID would like to respectfully suggest that the FERC order is a step in the right direction but did not fully consider all of the potential physical attacks that could cause 'widespread instability, uncontrolled separation, or Cascading within an Interconnection' or impair long term reliability of the system. MID feels that in responding to the FERC order, it would be acceptable to 'do the right thing' and step up to the challenge and evaluate all facilities identified in CIP-002-5 as high or medium impact the system against possible physical attacks.
New Brunswick Power Corporation	No	New Brusnwick Power (NB Power) agrees with the "applicability section" but not with portions of the preamble above, in question 1, which expands beyond applicability and states that "Furthermore, the standard drafting team expects many who are "applicable" to the standard will not identify facilities through their Requirement R1 risk assessment and Requirement R2 verification that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection." To our knowledge there is no evidence to support the standards drafting teams statement that they expect that many of the applicable entities will not identify facilities through R1 and R2. FERC's statement that "we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System" is not sufficient evidence. NB Power is concerned that the cost impact of this standard may be underestimated as a result of this view that the number of critical facilities will be small. Please see comments below with respect to R1 and R2.
Rayburn Country Electric Cooperative	No	Overall comment is this is too complicated of a draft standard for a 90 day consensus!Keep it simple. I agree with the functional entitiy that is identified however, I would add GO to address any "critical" switchyards that may exist that are not owned by a TO.I also agree with the scoping of the facilities similar

Organization	Yes or No	Question 1 Comment
		to the CIP V5 criteria with the following exception, apparently a list already exists for the substations that should be considered "high" do they deserve an alternative approach to what is within this standard?Altering the existing basic approach as follows:Since the FERC order allowed for “One or More Reliability Standards”, it would be appropriate to address the “High “ facilities separate from the “Medium Facilities”. This approach would make it an easier task to file the “high standard” within the 90 days then follow with the “medium later”. Thus giving more time, latitude and maneuverability to address issues that arise specific to those facilities.
Con Edison and Orange & Rockland	No	Reliability Coordinator, Planning Coordinator and Transmission Planner should be added to the Applicability Section. That will obligate these entities to meet the 90 day review period stipulated in R2.2, if they are identified as a verifying entity by the Transmission Owner.
Clark Public Utilities	No	Section 4.1.2 of the Applicability section states “Transmission Operator.” This reference in the Applicability section should be more specific based on the the actual conditions under which CIP-014 would be applicable to a Transmission Operator. Clark suggests the referense should be revised to “Transmission Operators that have operational control over the primary control center of a Transmission station or Transmission substation identified in section 4.1.1.”
Southwest Power Pool Regional Entity	No	SPPRE does not agree with the applicability because it excludes certain facilities that could pose a significant risk to the BPS reliability if rendered inoperable or damaged as a result of a physical attack. Other facilities that should be applicable are those where high impact BES Cyber Systems are found. Additionally, any Special Protection System and automatic load shedding system capable of shedding 300 Mw or more should be included. Reference CIP-002-5 Attachment 1 (Impact Rating Criteria 1.1, 1.2, 1.4,2.9, and 2.10). SPPRE also

Organization	Yes or No	Question 1 Comment
		disagrees with the decision to limit applicability to only the primary control center.
National Rural Electric Cooperative Association (NRECA)	No	Stations and substations should be clearly understood within the standard, not just through a guidance document or rationale. It is NRECA's understanding that a "station" equates to a switchyard that does not include transformers; and a "substation" is a facility that does include transformers. This should be addressed at the beginning of the standard document to ensure clear understanding throughout the standard.Do stations and substations focus only on certain key assets or all assets within the facility? Some assets could be those used for local distribution and/or be below 100kV. Clarity on this is required in order to understand the full scope and appropriateness of the standard.
Northeast Power Coordinating Council	No	The applicability of the draft standard should be expanded to incude Planning Coordinators in addition to Transmission Owners and Transmission Operators. While NPCC agrees that TOs and TOPs simple application of the screening criteria to determine which facilities need analysis, they may not be able to conduct a complete analysis. The SDT should consider that Transmission Owners in some cases do not have the ability to conduct an analysis with a "wide area" view of consequences. Smaller TOs or TOPs only have an outside equivalent representation of the BES and could need help conducting their analyses. Consideration should be given to allow them to conduct the studies in conjunction with PCs.
EF Cass Consulting Inc.	No	the applicability section table should be modified by either removing the 500kV line or making it a 3000 value. By giving it a 0 value in the table it send a different message than the text indicating all 500kV facilities are in. Also, in the draft RSAW Compliance Assessment approach for R1, it would appear that a Transmission Owner needs to comply with R1 and R2 in order to determine if the standard applies to them. If an entity is required to have a process for determining applicability then it needs to be a requirement. The applicability

Organization	Yes or No	Question 1 Comment
		section should produce a yes or no answer. I spoke with Nick Webber of WECC and his response back was "Much like the requirement of all entities to apply CIP-002, all entities registered as for the TO function must complete CIP-014-1 R1 and R2. Each TO must complete R1 to determine if R3-R6 apply. The TO then must subsequently have that R1 assessment reviewed as required in R2." An entity should not have to comply with 2 of the requirements in order to determine if the standard applies to them. If all TOs are expected to comply with R1 and R2, then move the criteria into the requirement, if that is not the intent, clarify that once an entity reviews the applicability section and determines the standard does not apply they are finished. The rationale for requirement R1 indicates the criteria is in R1 when it is actually in the Applicability section.
Bureau of Reclamation	No	The Bureau of Reclamation (Reclamation) believes that the Transmission Planner, Planning Coordinator, and Reliability Coordinator should be included in the Applicability section of the standard and should be responsible for reviewing the Transmission Owner's risk assessment (BES impact assessment).
Tri-State Generation and Transmission Association, Inc.	No	The drafting team may want to consider language referencing the CIP-002 Critereon rather than outright copying it in order to prevent changing multiple standards as the CIP-002 standard evolves.CIP-002-5.1 Attachment 1: Overall Application gave guidance on how to treat joint ownership facilities. Tri-State feels that this new standard would also benefit from such guidance.
Omaha Public Power District	No	The Omaha Public Power District (OPPD), suggests replacing the term "primary control center", using the NERC defined term "Control Center", with "primary Control Center".
NCPA Compliance Management Operating Committee	No	The Standard Drafting Team (SDT) estimates that relatively few Transmission Owners (perhaps 30 or less) will have Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability or uncontrolled separation. The Applicability section creates a lot of

Organization	Yes or No	Question 1 Comment
		work for many TOs an TOPS to identity those 30 or less transmission stations out of the 55,000 substations. The SDT might consider a higher level of applicability as was done for EOP-010-1, Geomagnetic Disturbance Operations i.e. apply the standard to Reliability Coordinators (RC) and only the Transmission Operators the RCs deem critical.This would be a more efficeint filtering process. Benefits of such an approach would be (1)Simplification and tighter security of critical information and informaton sharing (2) streamling and simplicaton of requirements for unaffiliated third party review, for example one reviewer could handle the risk assessment, vulnerability and threat assessment and review of security plans (combines requirements R2 & R6 together) (3)Time and resources of the entity could be more efficiently and economically managed as all reviews could be handled by a single Reviewer in a continuous manner rather than starting a stopping for different phases. (4) Saves many entities who would fall out of the process after going through the first three requirements. I expect RCs, ISOs and Regional Entities already know this
Kansas City Power & Light	No	There is a use of the term "critical" being used in several NERC Standards, which can cause unintended confusion. Since the applicability of this draft Standard is derived from the approved CIP-002-5.1, can this proposed Standard be added as a revision to CIP-002-5.1?
Utility Services	No	We have seen in the previous versions of the CIP standards that “Risk Assessments” are not performed consistently, and create more problems than they solve, and even violation determinations. The solution in CIP-014 to this inherent problem seems to just add another level of review, but there is no guarantee of consistency within these assessments. Additionally, it seems the drafting team is suggesting a single assessment (“Concurrent with R1 study” specified in R2), this this might eliminate the review stage all together. A clear applicability section with a “brightline” approach would be more appropriate and consistent with the progression of the CIP standards overall. Otherwise, what prevents an auditor from making a determination that the assessment

Organization	Yes or No	Question 1 Comment
		performed was not sufficient or incomplete, even with a 3rd party validation? Entities need a clear definition to avoid the problems of the past. If the drafting team wants to limit the scope of Facilities this could be detailed in the "Exemptions" portion of the "Applicability" section of the standard. 1. The "Exemption" section needs to be clarified. If this applies to the entire section number it 4.2. If it is only applicable to the last bullet it is under give it the appropriate number (4.1.2.1)Suggested re-write4. Applicability:4.1. Functional Entities:4.1.1 Transmission Owner4.1.2 Transmission Operator4.2. Applicable Facilities: The following Facilities, systems, and equipment, owned or operated by each Responsible Entity in 4.1 above are those to which these requirements are applicable. 4.2.1 Transmission Facility operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.4.2.2 Transmission Facility that operate between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.ADD TABLE HERE4.2.3 Transmission Facility at a single station or substation location that is identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.4.2.4 Transmission Facility at a single station or substation whose unplanned unavailability would result in the loss of at least 3000 MW of generation.4.2.5 Control Center that controls:4.2.5.1 Transmission Facilities identified by

Organization	Yes or No	Question 1 Comment
		identification under 4.2.1 through 4.2.4; or4.2.5.2 Two or more Facilities which contain a Cyber System(s) which have been identified as a High or Medium Impact BES Cyber System.4.2.6 Exemptions: 4.2.6.1 All facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission.4.2.6.2 Transmission station or substation connected to only one other Transmission station or substation.4.2.6.3 Transmission station or substation that does not operate above 200kV.4.2.6.4 control centers not designated as a "primary control center"
SPP Standards Review Group	No	We have some concern with the undefined term 'collector bus facility'. Without a definition for collector bus facility some may consider the entire switchyard at a generating station as a collector bus facility. We do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
Public Utitliy District No. 1 of Cowlitz County, WA	No	We strongly disagree with applicability statements being outlined in the requirement. We support APPA's recommendation to further define TOP applicability in section 4.1.2 to avoid nuisance compliance certifications.
Western Electricity Coordinating Council	No	WECC questions why generation assets are exempt from analysis and verification required by Requirements R1 and R2. It is possible that some generation assets, if rendered inoperable, could result in widespread instability, uncontrolled separation, or Cascading.WECC recommends removing the 500 kV line in the Weighted Value table. All 500 kV facilities are to be assessed per Applicability Section 4.1.1.1 and including 500 kV lines in the table in applicability section 4.1.1.2 with a zero value seems more likely to add confusion than to provide clarifying information.Applicability section 4.1.2 makes it look like the standard is applicable to all Transmission Operators. WECC suggests adding some clarifying language to indicate that the standard is only applicable to Transmission

Organization	Yes or No	Question 1 Comment
		Operators notified per Requirement R3. This may serve to make the standard more acceptable to Transmission Operators in general.
Herb Schrayshuen	No	The applicability of the standard is to Transmission Owners and Transmission Operators. Generating plants sites where the facilities production capability exceeds 1000 MW or other suitably larger amount should be included.
Bonneville Power Administration	Yes	4. Applicability: BPA believes that the medium list for HV transmission entities will result in numerous facilities having to be protected (all 500 kV) contrary to the drafting team comment that not many facilities will be deemed critical. 4.1. Functional Entities: BPA recommends that this section reference the criteria of CIP-002-5.1 for a "medium impact rating," instead of re-stating it without citation. Otherwise it is confusing. For example, the source of the tabulated weighting criteria is unclear and it is difficult to know there is a connection to any previous or established standards.
Idaho Power Co.	Yes	4.1.2. Seems vague in its description lending the reader to believe that TOPs are in scope at all times which is inconsistent with guidance later in the standard which states they are only required to perform actions when informed they are in scope by a TO. Further Clarification is needed in this section.
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.CONTROL CENTER - Use the defined term "Control Center" by capitalizing as "primary Control Center" or explain why lower case "primary control center" is different and needs to be used in the standard. Consider inserting "with operational control" after primary Control Center, to express the intent of the text box Rationale for Requirement R1 that the control center must be capable of taking

Organization	Yes or No	Question 1 Comment
		electronic actions that can cause direct physical actions at the identified station or substation. Please also clarify whether the periodic use of a backup control center as the entity's primary control center would make R4 and R5 applicable to both the primary and backup control centers.UNAFFILIATED - needs to be either defined or a footnote needs to be added to the standard to explain that "unaffiliated means that the selected verifying or reviewing entity cannot be a corporate affiliate," as stated in the guidance section.CONFIDENTIALITYPublicly Owned Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the A. Introduction section, after 6. Background:7. Critical Facilities InformationRecords and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments

Organization	Yes or No	Question 1 Comment
		and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. ALTERNATIVE PROPOSED REQUIREMENT LANGUAGE ADDITIONS:R1.3 The Transmission Owner will keep confidential all records and information related to the risk assessments conducted under this standard.R3.2 The Transmission Owner will keep confidential all records and information related to the notifications conducted under Requirement R3 and R3.1 of this standard. R4.4 The Transmission Owner and each applicable Transmission Operator will keep confidential all records and information related to the evaluation of physical threats and vulnerabilities to each of its transmission substation(s) and primary Control Center(s) identified in Requirement R1. APPA suggests technical edits to Requirements R2.4 and R6.4 to insert "or made available to" after "exchanged with." This change would clarify that sensitive or confidential information does not have to be actively "exchanged" between entities to be subject to the protections directed under Requirements R2.4 and R6.4. APPLICABILITY 4.1.2 - The applicability section for Transmission Operators under section 4.1.2 should be explicitly limited to each TOP that operates a primary Control Center and receives a verified notification under Requirement R3. As written each TOP would be required to certify on each compliance contact that it has not been notified that it operates an applicable primary control center. The following edited text would accomplish that objective:4.1.2 Transmission Operator that operates a primary Control Center and receives notice from a Transmission Owner under Requirement R3.Please also confirm that the Transmission Operator of a primary control center is not responsible for conducting a risk assessment under R1 or arranging for third party verification of the risk assessment under R2.

Organization	Yes or No	Question 1 Comment
The Empire District Electric Company	Yes	EDE feels this is the right approach on selecting a threashold for applicability to this standard.
ISO/RTO Standards Review Committee	Yes	IntroductionThe proposed standard provides adequate flexibility with respect to the risk assessments and security evaluations and plans. This allows the industry to capitalize on their experience in these matters, while also accommodating changes that warrant consideration. Applicability SectionThe applicability scope is reasonable in terms of identifying the appropriate functional entities to address physical security concerns. Similarly, the proposed standard establishes a reasonable approach for identifying the scope of facilities by 1) initially defining an objective set based on the CIP-002-5.1 criteria, and then 2) refining that set based on analyses that assess the relationship of those facilities to specific, system conditions/impacts metrics - i.e. widespread instability, uncontrolled separation, or Cascading within an Interconnection.
National Grid	Yes	It should be clear that the applicability section of the standard is only intended to provide a valid, technically sound basis to be used as the 'starting point' to those transmission facilities or stations that should be included in the risk assessment.We suggest the following modifications:4.0 Applicability:4.1 Functional Entities:4.1.1 Transmission Owner that owns any facilities identified in the following sections (4.1.1.1 through 4.1.1.4) will be required to perform the risk assessment and risk assessment validation as outlined in R1 and R2 of this standard. Should the risk assessment identify critical assets then the Transmission Owner is subject to the remaining requirements (R3 through R6) of the standard. 4.1.2 Transmission Operator
ITC	Yes	ITC agrees with utilizing, as a starting point, the CIP-002-5.1 "medium impact" rating to determine the facilities needing enhanced physical security. As ITC indicated in its comments to FERC in Docket No. RD14-6, these new physical security Standards must be developed in a coordinated manner to avoid

Organization	Yes or No	Question 1 Comment
		duplicative, overlapping, or contradictory requirements among the various existing Reliability Standards that cover a similar if not an identical set of assets. By ensuring "that entities could apply the same set of criteria to assist with identification of facilities under CIP Version 5 and proposed CIP-014-1," the SDT has fully met our expectations with respect to the applicability of the standard.
Los Angeles Department of Water and Power (LADWP)	Yes	LADWP requests the Drafting Team to make the following changes:- For Secion 4, you may want to add Transmission Planner and Planning Coordinator to the applicability. These functions may have responsibility on at least R1 and R2.- Secion 4.1.1.1 - Add "(AC or DC)" as follows: "Transmission Facilities operated at 500 kV (AC or DC) or higher....."
Public Utility District No. 2 of Grant County, WA	Yes	Language contained in R1 does not align the performance of risk assessments of Transmission stations and Transmission substations with the actual commissioning or energization of such facilities. To ensure that risk assessments and subsequent risk assessments address existing and planned Transmission stations and Transmission substations to be in service within a risk assessment window the following edits are recommended to R1:R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months) ..1.1. Subsequent risk assessments shall be performed at least once every 30 calendar months. (this would apply to all applicable TOs) GCPD also supports comments made by APPA regarding the insertion of the language addressing Confidentiality and treatment of Critical Facilities Information. GCPD's suggested language is as follows: Risk assessments and evaluations of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access, and any organization or agency charged with examination of such records and information pursuant to

Organization	Yes or No	Question 1 Comment
		Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure.
MidAmerican Energy Holding Company	Yes	MidAmerican Energy Holdings Company (MEHC) agrees with the applicability section.
MISO	Yes	MISO supports the proposed applicability section and agrees that other entities do not need to be included. In particular, MISO would not support application of this Standard to Reliability Coordinators or Balancing Authorities, as these entities' control centers are adequately protected with regard to physicial security under CIP-006-3c and its successor standard. Moreover, these control centers are subject to the requirements of EOP-008-1 including the transfer functional control to backup facilities. MISO therefore agrees that the focus of CIP-014-1 should be those facilities that are not otherwise fully protected by CIP-006-3c, such as those that do not not rely entirely on Critical Cyber Assets to maintain reliability.
ATCO Electric	Yes	No Comment.
SERC CIPC	Yes	Recommend that the drafting team include the Transmission Planner who would be performing the risk assessment in the applicability as discussed in R1.
ReliabilityFirst	Yes	ReliabilityFirst supplies the following comments for consideration:1. ReliabilityFirst believes there may be a perceived disconnect between the Applicability Section and Requirements 5 and 6. Requirements 5 and 6 introduce new requirements surrounding the Transmission Owners "primary control center" though the "primary control center" is not listed within the Applicability section as an asset the Transmission Owner owns that is included in the standard. Consideration may be given to adding "primary control center" under section 4.1.1. [Note: Since "Control Center" is a NERC defined term, this term should be capitalized throughout the standard.]2. Applicability section 4.1.1.4 -

Organization	Yes or No	Question 1 Comment
		ReliabilityFirst believes the term “as essential” is ambiguous and may cause unintended compliance monitoring implications. ReliabilityFirst recommends the following for consideration: “Transmission Facilities identified [in] Nuclear Plant Interface Requirements [which provide offsite power].” ReliabilityFirst believes the recommended language addresses the intent of the SDT.
San Diego Gas & Electric	Yes	San Diego Gas & Electric (SDG&E) agrees that it is appropriate to start with those Transmission Owners that own Transmission facilities that meet the bright line criteria in Reliability Standard CIP-002-5.1 for a “medium impact” rating. However, SDG&E believes that it would be prudent to simply refer to the CIP-002-5.1 Impact Rating Criteria rather than restating it in CIP-014 Standard. Being more specific that this Standard is applicable to Transmission Owners that have any facilities identified as “medium impact” facilities under CIP-002-5.1 Attachment 1, Inpact Rating Criteria 2.4, 2.5, 2.6 and 2.7, would be clearer and more consistent with the general way that CIP-003-5 through CIP-011-5 are built upon the identification of “critical” facilities made in CIP-002-5.1. Linking the two explicitly, rather than simply restating the same language, would prevent the possibility that differences could creep into the rules over time as each Standard is modified.
Seattle City Light	Yes	Seattle City Light supports the Question 1 comments of APPA, with one exception in the area of Confidentiality. Seattle's comments about Confidentiality, in place of APPA's comments on this topic, follow.CONFIDENTIALITYThe stated purpose of draft CIP-014-1 Physical Security is: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Public Utilities subject to state Open Records Acts are concerned that records produced, gathered, used and maintained as evidence of compliance with this standard may be subject to disclosure under applicable state laws. To protect this critical

Organization	Yes or No	Question 1 Comment
		information from disclosure, we suggest adding a provision to the Introduction section of the proposed standard that designates the produced, gathered, used and maintained records related to compliance with this standard as exempt from disclosure. Alternatively, we suggest the addition of Requirements to protect the records and information from disclosure. Proposed language for a new #7 in the Introduction Section:7. Critical Facilities InformationRecords and related information concerning critical facilities physical infrastructure, including risk assessments and evaluation of physical threats and vulnerabilities, as produced, gathered, used or maintained for compliance with mandatory Reliability Standards, are intended to be kept confidential by the owner of the records and information, those entities with authorized access to the records and information, and any agency charged with examination of such records and information pursuant to Section 215 of the Federal Power Act. All such identified records and information are also intended to be exempt from public disclosure. Consistent with that premise, the purpose of the cyber and physical security Reliability Standards are to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or cascading within an interconnection. Consequently, records and information detailing the physical infrastructure, including records and information related to the risk assessments and evaluation of physical threats and vulnerabilities conducted under this Reliability Standard and all records and information produced, gathered, used and maintained for compliance with this Reliability Standard shall be considered critical facilities information and are intended to be exempt from disclosure under public records laws. Nothing in this section or the Reliability Standards is intended to eliminate other lawful methods of access to such records and information. Proposed Requirement Language:R1.3 Records and information related to the risk assessments conducted under this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure.R3.2 Records and information related to the risk assessments conducted under

Organization	Yes or No	Question 1 Comment
		Requirement R1 of this standard that are designated confidential by the Transmission Owner are [intended to be] exempt from public disclosure. R4.4 Records and information related to the evaluation of physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and/or Control Center(s) identified in Requirement R1 conducted under this standard that are designated confidential by the Transmission Owner or Transmission Operator are [intended to be] exempt from public disclosure.
Arizona Public Service Company	Yes	See related comments under Requirement 2 below.
Seminole Electric Cooperative, Inc.	Yes	Seminole supports the comments by NRECA. Additionally, Seminole supports the use of CIP-002-5 medium impact criteria for use in CIP-014. CIP-002-5 has at least one issue that will apply to CIP-014 as well. There are multiple ways to interpret the phrase Transmission Facility. One example is clarifying what is in the scope of a Transmission Facility. The definition or other documentation should state that the substation is exclusive of the criticality of any connected substation and clarify that a Transmission Facility as used here does not include Transmission Lines.
Salt River Project	Yes	SRP supports comments submitted by APPA.
Northeast Utilities	Yes	Standard Drafting Team should define the term widespread. NU suggests the following definition:Widespread - An event that causes voltage collapse, Cascading and/or instability that results in uncontrolled separation across significant portions of the Interconnection. The registered entity shall use regional criteria to evaluate.
PNM Resources	Yes	Support the comments submitted by EEI.
Texas RE	Yes	The applicability should include the TP, PC, RC, and the unaffiliated entity as they are noted in this standard.

Organization	Yes or No	Question 1 Comment
PPL NERC Registered Affiliates	Yes	These comments are submitted on behalf of the following PPL NERC Registered Affiliates: Louisville Gas and Electric Company and Kentucky Utilities Company; PPL Electric Utilities Corporation, PPL EnergyPlus, LLC; PPL Generation, LLC; PPL Susquehanna, LLC; and PPL Montana, LLC. The PPL NERC Registered Affiliates are registered in six regions (MRO, NPCC, RFC, SERC, SPP, and WECC) for one or more of the following NERC functions: BA, DP, GO, GOP, IA, LSE, PA, PSE, RP, TO, TOP, TP, and TSP.The PPL NERC Registered Affiliates support the draft standard. As members of EEI, we also support the comments being submitted by EEI. In addition, we have provided specific comments that we believe would add clarity to the standards and simplify the requirements. We urge the SDT to consider our comments and incorporate them as appropriate when developing the final standard that will be balloted. Comments: Section 4.1.1.2 includes in the applicability Transmission Owners that own Transmission Facilities that are operating between 200kV and 499 kV at a single station or substation, where the station or substation is connected at 200kV or higher voltages to three or more other Transmission stations or substations and has an "aggregated weighted value" exceeding 3000 according to the table set forth in section 4.1.1.2. Because section 4.1.1.1 covers transmission facilities operated at 500 kV and above and section 4.1.1.2 only references Facilities operating between 200 kV and 499 kV, the fourth row in the table in section 4.1.1.2 referencing voltages of "500kV and above" is unnecessary and should be removed.
NRG Energy, Inc.	Yes	This standard should not address generation interconnection facilities because the BES is designed to withstand the loss of generation facilities through the use of regional reserves.
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	Yes	Vectren supports the use of the CIP-002-5.1 medium impact criteria. This approach focuses on the facilities that could have a true adverse impact to the Bulk Electric System and provides consistency with approved standards.

Organization	Yes or No	Question 1 Comment
Hydro One	Yes	We agree with the Applicablity. R1 has provided flexibility in the assessment method.
Independent Electricity System Operator	Yes	We agree with the inclusion of the Transmission Owners and Transmission Operators as they have the obligations to conduct an evaluation of the potential threats and vulnerabilities to a physical attack on each of their respective transmission stations/control centres.
ACES Standards Collaborators	Yes	We support a clear and defined “bright line” criteria that has been industry vetted and FERC approved as the starting point for the risk assessment in R1.
Cooper Compliance Corp	Yes	We support the applicability proposed by CIP-014-1.
Western Area Power Administration	Yes	Western agrees with what we understand as the applicability, based on the CIP-014 Workshops. However, we have some concern with the undefined term ‘collector bus facility’. Without a definition for collector bus facility we are concerned that some parties may consider the entire switchyard at a generating station as a collector bus facility. Based on the discussion during the CIP-014 Workshops we do not believe the drafting team intended this to be the case. Therefore, some additional clarification may be needed for the term.
Vermont Transco LLC	Yes	While we do agree with the need for the standard and the importance of it we do have comments on the proposed standard. The intention of this standard is to protect those facilities that are most critical to the bulk electric system. The CIP-002-5.1 criteria brings into play many facilities that while deemed critical to an entity are not likely critical to this standards definition and would not cause wide area impact.
Consumers Energy Company	Yes	With Michigan situated as a peninsula, Michigan infrastructure may be at a lesser risk, based on the limited number of interconnect avenues into and out of our system. Meaning the highest level of criticality likely would be identified as

Organization	Yes or No	Question 1 Comment
		those key interconnect points, and not the entirety of our system. From our experience with the blackout of August 2003, BES implications were centered in southeast Michigan and although affected, we were able to successfully minimize/sustain our base load generation requirements. Any substation targeted in Michigan may not have a cascading effect on the BES.
Dominion	Yes	
Duke Energy	Yes	
FirstEnergy	Yes	
Florida Municipal Power Agency	Yes	
Tampa Electric Company	Yes	
Tennessee Valley Authority	Yes	
Ameren	Yes	
American Electric Power	Yes	
American Transmission Company, LLC	Yes	
Basin Electric Power Cooperative (BEPC)	Yes	
California ISO	Yes	

Organization	Yes or No	Question 1 Comment
Central Hudson Gas & Electric Corporation	Yes	
City of Garland	Yes	
Colorado Springs Utilities	Yes	
Edison Electric Institute	Yes	
Empire District Electric Company	Yes	
Exelon	Yes	
Flathead Electric Cooperative, Inc.	Yes	
FortisBC	Yes	
GridWise Alliance	Yes	
Hydro QuÃ©bec TransÃ‰nergie	Yes	
Manitoba Hydro	Yes	
Minnesota Power	Yes	
Minnkota Power Cooperative	Yes	
None	Yes	
Pacific Gas and Electric Company	Yes	

Organization	Yes or No	Question 1 Comment
Peak Reliability	Yes	
Pepco Holdings Inc.	Yes	
Portland General Electric	Yes	
South Carolina Electric and Gas	Yes	
Southern California Edison Company	Yes	
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	
The Empire District Electric Company	Yes	
Virginia State Corporation Commission	Yes	
Westar Energy	Yes	
Xcel Energy	Yes	
Encari		Historically, FERC and NERC have taken the position that redundancy is not an acceptable criterion to exempt a Critical Cyber Asset from mandated physical or

Organization	Yes or No	Question 1 Comment
		cyber controls. Redundancy is not supposed to be a factor in the determination of the criticality; instead redundancy is used to improve reliability and availability. This principle should be extended to the protective measures applicable to control centers under CIP-014-1. So long as both the primary control center and backup control centers meet the bright line criteria for a medium impact rating under CIP-002-5.1, the protections under CIP-014-1 should apply equally to both the primary and backup control centers.
APPA		SMUD supports the APPA comments and is specifically concerned that records and information developed and maintained under each of the requirements for this standard are afforded the necessary protection through an introduced section, #7 Critical Facilities Information. We respectfully ask the Standard Drafting Team to ensure that AUTHORIZED ACCESS to information pertains to ANY RECORD AND INFORMATION associated with the Physical Security Standard.

2. **Requirements R1 through R3: The first three requirements of CIP-014-1 require Transmission Owners to: (1) perform risk assessments to identify through transmission planning analysis those Transmission stations and Transmission substations that meet the "medium impact" criteria from CIP-002-5.1, and their associated primary control centers, that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; (2) arrange for a third party verification (as directed in the order) of the identifications; and (3) notify certain Transmission Operators of identified primary control centers that operationally control the identified and verified Transmission stations and Transmission substations. The requirements provide the periodicity for satisfying these obligations. Only an entity that owns or operates one or more of the identified facilities has further obligations in Requirements R4 through R6. If an entity identifies a null set after applying Requirements R1 through R2, the rest of the standard does not apply. Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security**.

Summary Consideration: The SDT thanks all commenters. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Requirement R2, Part 2.2 was reworded to align with the intended applicable entity. Language was added to Requirement R2, Part 2.4 to specify that the TO must develop procedures to protect or exempt sensitive or confidential information developed pursuant to the standard from public disclosure. A change was made to Requirement R3 to accurately state which primary control centers are included in the requirement. Corresponding changes were made to each measure. Several additions and clarifications were made to the Guidelines and Technical Basis section based on stakeholder comments. A summary of comments and the SDT's response is provided:

- **Requirement R1. Commenters suggested removal or changes to the term 'Risk Assessment' in R1.** The SDT maintained language consistent with the FERC Order.
- **Requirement R1. Commenters recommended additions to the Guidelines and Technical Basis section to clarify the term 'primary control center'.** The SDT has added language to the Guidelines and Technical Basis section to clarify a primary control center.
- **Requirement R1. Commenters asked for clarification on the type of analysis required for a risk assessment, recommended specific TPL approaches, proposed N-1 analysis for long lead time replacement equipment, and recommended use of IROL criteria.** The SDT has written the requirements to allow flexibility for the TO to include risks that it believes are realistic. The resulting physical security plan is to be designed to protect the assets, including any long lead-time assets. Specifically, in Requirement 5, Part 5.1, the standard identifies resiliency as an appropriate consideration when drafting a physical security plan. A TO may use IROL criteria but the SDT intends for the standard to provide flexibility.
- **Requirement R1. Commenters suggested alternate periodicity.** The SDT believes the specified periodicity is reasonable and will identify assets in a timely manner. The SDT notes that the periodicity is aggressive but achievable. The SDT considered a balance

of risk to the BPS and burden to the responsible entity when developing the periodicity. If the TO does not identify Transmission station or Transmission substation in its risk assessment, then the periodicity changes to 60 months.

- **Requirement R1. A commenter suggested removing the requirement to include facilities that are planned to be in service within 24 months and replacing it with a requirement to update the risk assessment prior to addition of a new Transmission station or Transmission substation.** The SDT chose the language of R1 so that entities would have a fixed starting point for risk assessment of existing stations as well as those planned to be operational within 24 months from the assessment date. The TO may perform additional assessments prior to adding facilities as the standard does not preclude additional assessments. Verification of additional risk assessments conducted more frequently than the periodicity prescribed in the standard is not required.
- **Requirement R2. Commenters recommended removing third party verification, changes to entities in Requirement R2, Part 2.1, additions of PC, TP, and RC to the applicability, limiting verification to the Regional Entities based on confidentiality concerns, or not permitting the same organization that conducted the risk assessment in Requirement R1 to be a verifier.** The third party verifier and reviewer are specified in the FERC Order. The SDT believes its approach with verifiers and reviewers is consistent with the FERC Order. The SDT believes the most reliability benefit will come from providing flexibility to TOs rather than adding prescription, even for purposes of making compliance easier. The SDT discussed many options with respect to the risk assessment and the confidentiality of information. The team reached consensus with the proposed requirements that provide flexibility in who performs the risk assessment and verifications while protecting the confidentiality of information.
- **Requirement R2. Commenters indicated that the term 'unaffiliated' was not sufficiently clear. Federal government-owned entities stated the SDT's definition of unaffiliated could exclude other agencies.** The Guidelines and Technical Basis section explains the SDT's use of the term unaffiliated. It was amended to more clearly indicate that a government-owned utility could use another government entity to satisfy the verification required by R2. The following was added: "The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit."
- **Requirement R2. Commenters indicated additional guidance on protecting sensitive or confidential information was needed.** The Guidelines and Technical Basis section has been revised to address the concern. Please see response to this concern in Question 1 above.

- **Requirement R2. A commenter asked the SDT to clarify whether third party verification was required for a minor revision to the Requirement R1 risk assessment.** As stated in the requirements, the risk assessment shall be performed at least once every 30 calendar months (or 60 calendar months if no assets were identified in the previous risk assessment) and verified within 90 calendar days of completion. Entities are not precluded from performing additional actions outside the context of the standard requirements.
- **Requirement R2. Commenter proposed alternate language to Requirement R2, Part 2.2 to be consistent with applicability of the standard.** The SDT agreed and made this clarifying change.
- **Requirement R2. Commenters suggested changes to requirements for documenting recommendations from the third party verifier.** The SDT believes it is appropriate to document the TO's response on all recommendations from the verifier, even if the verifier is recommending the removal of an asset from the list developed in Requirement R1.
- **Requirement R2. Some commenters indicated the timeline was too short.** The SDT believes the timeline is aggressive but achievable and further supports stakeholder consensus.
- **Requirement R3. A commenter proposed adding clarification to the Guidelines and Technical Basis section on what operational control means.** The SDT has added a description to the Guidelines and Technical Basis section.
- **Requirement R3. A commenter stated that 7 days was an unnecessarily short timeline.** The SDT believes that the notification is important for reliability since the necessary subsequent actions for developing a security plan may not be triggered until the notification has occurred.

Organization	Yes or No	Question 2 Comment
ACES Standards Collaborators	No	(1) Conceptually, we agree with this approach but have identified the following issues and concerns. (2) R1 requires additional clarification. The Guidelines and Technical Basis section states that the "bright line" criteria in applicability section is used to identify an initial set of stations and substations that must be further evaluated in R1. It is our understanding that if a TO owns one 500 kV transmission station and no other transmission facilities, then that 500 kV station would meet the applicability section 4.1.1.1 criteria. The TO would be required to perform a risk assessment to identify if that facility was rendered inoperable, it could result in widespread instability, uncontrolled separation, or Cascading in an Interconnection. In other words, if the applicability section is met, the TO must perform a risk assessment, but the remainder of the standard (R4-R6) would not apply unless loss of the Facility would result in widespread instability, uncontrolled separation or Cascading. Please confirm if our understanding of applying the requirements is the correct approach. (3) We see a significant compliance risk created by Requirement R2 and question why the unafilliated third party verification cannot be integrated into the Regional Entity compliance monitoring and enforcement processes to minimize costs and limit access to highly sensitive information. The third party verification creates a compliance problem outside of the TO's control because the TO is dependent on a third-party for regulatory compliance and there is no obligation on any of the third parties (i.e. RC, PC) identified in the standard to verify the risk assessment. Thus, the TO will have to rely on consultants to perform the verification. Since all TOs will be working towards the same efffective date, there will be a backlog and the reviews may not be completed by the timelines established in the standard. Review by consultants also will increase the number of people with access to highly sensitive information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. All of these issues could be resolved if NERC and Regional Entities conducted the review. The review could be performed as part of a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or

Organization	Yes or No	Question 2 Comment
		believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolved the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. As an alternative, we suggest that a companion requirement that compels either the RC or PC to perform the verification. This would also reduce the costs impacts and distribution of sensitive information since these entities will already be familiar with the TOs they are verifying and will already have access to highly sensitive information. (4) Regarding R3, this requirement does not warrant a 7-day timeline. This is not a near real-time issue. We suggest 30 days as a reasonable notification period.
Ameren	No	(1) Regarding R3 and R3.1, we believe that the 7 day requirement is too short and 30 days would be more appropriate to notify other utilities. (2) R4 should have wording added to the requirement that the R4 evaluation is to be completed 120 days after the completion of R2. Then, the R5 wording should be changed so that the R5 physical security plans should be completed 120 days after the R4 evaluation is completed.
Utility Services	No	1. What is a Transmission "station"? What is the definition of station and what is it intended to cover that substation does not. Generally in the NERC glossary "station" is associated with Generation, not Transmission. 2. There is a concern between R1 and R5. a. R1 states that substations planned to be in service within 24 months should be identified, which would presumably be for stations under construction. b. R5 will then require a Physical Security plan to be in place within 120 days of identification, regardless of the current status of the station. c. Possibly adjust language to allow sites under construction to have the later of 120 days or the operation date of the station. 3. R1.2 should be reworded: "The TO shall identify the primary Control Center with operational authority of each Facility identified in the R1 risk assessment."4. R2, if the assessments are concurrent, could this be a joint effort, with the result being 1 report? 5. R2.1, "unaffiliated" needs some clarification. Is this unaffiliated with the TO in any way? Could the TO use their Planning Coordinator,

Organization	Yes or No	Question 2 Comment
		Transmission Planner or RC for the assessment, or do they need to seek out an entity from another region?
David Kiguel	No	1. For clarity suggest that the word “verify” be changed to “confirm” in sub-requirement 2.2 so that it reads: “The unaffiliated verifying entity shall either confirm the Transmission Owner’s risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s).2. Sub-requirement 3.1 should cover both, addition and removal of elements from the identified facilities list. Suggest changing to:”In the case of addition(s) to, or removal(s) from the identified Transmission stations or Transmission substations list developed under Requirement R1 and verified/modified according to Requirement R2, the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the change(s).”
Texas RE	No	1. For R1, the Transmission Owner is not the appropriate entity to conduct the type of transmission analysis that the requirement describes. It seems like a more logical process would be for the Transmission Planner to conduct an analysis of all substations meeting the applicability in 4.1.1.1 thru 4.1.1.4, and then, if the removal of a substation results in Cascading, instability, or uncontrolled separation, the TP will then notify the TO & TOP to conduct the security threat evaluation per R4 at only those substations identified by the TP.2. R1 - A “risk assessment” pertains to the physical security of Transmission Facilities while a “risk-based assessment” pertains to identification of Critical Assets and Critical Cyber Assets. The two phrases are too similar in meaning to each other, but possess differing meanings and intents.3. For R2, if the approach described in #1 is accepted, it may also satisfy R2 in those cases where the TP is independent from the TO. The independent verification would also be the responsibility of the TP, utilizing another TP, the PC, the RC, or an unaffiliated entity as described in the current language.4. For R3, if the approach described in #1 is accepted, the initial notification to the TOP would originate from the TP.

Organization	Yes or No	Question 2 Comment
South Carolina Electric and Gas	No	A) The FERC order directs that the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. It does not require verification of the specific or particular facilities identified. Therefore, SCE&G believes this section should be clarified and specifically state that the assessment itself (i.e. the methodology used by the owner or operator) be verified and not the facilities.B) SCE&G would like the drafting team to comment on the liabilities a NERC registered entity may assume as the third party when they are used to verify the risk assessment. Specifically, if in a future audit the owner or operator's assessment is found noncompliant, then would the independent NERC registered third party entity suffer any noncompliance as well? It is important for NERC registered entities to understand their compliance risks as third parties before they agree to perform independent verification of other entities assessments.
Florida Keys Electric Cooperative	No	o Comments: R1.1 - FKEC recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straight forward than a 2.5 year focus and it's easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement. o R2 - The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word "should," not "shall" or "require." The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what "verify" means in the standard. Guidance and rationale is helpful, but does not carry to legal weight of the standard language. o R2.1 - This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment

Organization	Yes or No	Question 2 Comment
		is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. o Are there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in theNERC facility ratings alert responses. o How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor.o If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired - this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard. o R2.2 - This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. o R2.4 - The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entity o R3.1 - The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. FKEC believes 30 days is more appropriate timeframe for this requirement.
Black Hills Corporation Entities	No	Although BHC agrees with the overall approach, it has significant concerns regarding the use of the term "risk assessment" without a clear definition of intent. CIP-002 regulatory expectations in the Western interconnect for RBAM have consistently referred to the classic risk definition as "risk" times "probability". However, the further

Organization	Yes or No	Question 2 Comment
		expectation is that the probability of an event is assumed to be 100%, such that the "risk" them becomes equal to the "impact". CIP-014 does not currently lay out the same expectations, which could allow Transmission Owners and other affected (or unaffiliated) parties to disagree over the role of "proabability" in defining risk.This problem can be resolved in the CIP-014 draft by:1. leaving the risk assessment language as is, but adding the above statements about "probability" of occurrence being 100%, or2. changing all references of 'risk assessment' in the standard, to 'impact assessment', or3. leave the risk assessment language as is, but make it clear that CIP-014 is deviating from the historical CIP-002 RBAM definition of risk, such that the probability of the event can change the perceived risk (and that such an interpretation is congruent with the FERC order. This last option seems to be closest to the intent of Paragraph 8 in the FERC directive, but represents a significant departure from past NERC CIP guidance, and needs to be highlighted as such.As written, the TO has exclusive determination say in identifying applicable Transmission stations, substations and primary control centers. R2 speaks to a third party verification of that assessment, but Black Hills believes that coordination of the BES would be better served by having the TO & TOP reach a consensus on the assessment, prior to having the assessment validated by a third party.Requirement 2.1 directs the Transmission Owner to select an unaffiliated Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. Firstly, Planning Coordinator does not appear in the NERC functional registry and should not be casually equated with the TP and RC functions; without first equating the Planning Coordinator to the PA function per the NERC glossary. Secondly, none of these NERC functional entity designations appear in the applicability section of the standard. Therefore, it can be assumed that the unaffiliated PC, TP, or RC are not obligated to conduct the assessment themselves, but rather the assessment is conducted by mutual agreement of the TO and unaffiliated PC, TP, or RC acting as third-party assessor. If this is not the correct assumption, then the PC, TP, and RC functions should be noted in the applicability section. If the Transmission Owner is affiliated with the Transmission Planner and Planning Coordinator, then the third-party review should be performed by the entity's Reliability Coordinator.The reference to "primary control center" is adequately

Organization	Yes or No	Question 2 Comment
		explained in the rationale section of R1, but confusion between it and “back-up control centers”, “emergency dispatch center”, and those control centers that can only monitor status seem to justify an up-front definition in the standard. Recommend that a special definitions section be added, or the term be clearly defined at its first instance in Section 3.R2.4 could benefit from some added guidance regarding the protection of sensitive or confidential information. Is the intent to employ the entity’s baseline confidentiality banner, or something more robust such as that required by CIP-003-3 R4 or CIP-011-1. The latter seems more appropriate for this CIP standard.
NCPA Compliance Management Operating Committee	No	Applicability is a key issue here. Comments to question 1 apply here as well. Why subject all Transmission Owners who may meet the "medium impact under CIP-002-5.1 to a third pary review for all medium impact stations and substations when only 30 stations will be affected (please define the difference between a Transmission station and Transmission substation. A third party review is appropriate for the 30 or so stations involved, but seems excessive for all owners to obtain third party review when the expectation is that 30 out of 55,000 are te ones of real concern. NCPA elected to have an independent third party risk asssessment and vulnerability assessment performed at its 5 generation facilities and control center. The assessment cost is approximately $150K and takes about 9 months to complete. NCPA'a assets are also low impact. The risk assessment, vulnerability and threat assessments and development of the security plans are able to performed by the same third party reviewer that flows together without interruption. The way in which the requirements are structured creates alot of consultants or third party reviewers running around, with 99% of them stopping work after R3. How much money will be spend for that and for what purpose? There has to be a better way segregate the 99% from the 1% where the real concern is.
Flathead Electric Cooperative, Inc.	No	Do not support the third party requirements, seems like a full employment effort by security consultants and others. Administratively burdensome and time-consuming at the expense of actual security improvements.

Organization	Yes or No	Question 2 Comment
Florida Municipal Power Agency	No	FMPA commends the efforts of the SDT to lay out an excellent process for risk assessment in accordance with the FERC Order in such a short time frame. We only have few comments. WHAT DOES “CONTROL CENTER” MEANIs there a signifance for not using the capitalized term of Control Center throughout the standard? It seems to FMPA that the defined term “Control Center” ought to be used. If the intent is that “control center” and “Control Center” mean two different things, then, what does “control center” mean? If the intent is to include large TOs that may be part of a large TOP, such as a large utility in an RTO, that do not have Control Centers; then, FMPA recommends using a different term such as “the location of the SCADA system that has remote control of breakers associated with the identified substation/station” or similar might avoid confusion.WHAT DOES “UNAFFILIATED” MEANThe term “unaffiliated” may be a source of ambiguity and conflict without further definition. For instance, dictionary.com defines affiliated as: “being in close formal or informal association; related” So, this would imply that peer members of the Transmission Forum are affiliated, which we do not believe is the intent of the SDT. FMAP believes the SDT’s intent is as Black’s Law Dictionary defines affiliate: “1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.”; which would mean that peers within the Transmission Forum are unaffiliated, but subsidiaries of a company are affiliated, or members of a Joint Action Agency are affiliated. It also aligns with FERC’s definitions for Affiliate in their market based rates regulations 18 C.F.R. 35.36(a)(9) and in the Pro Forma OATT. FMPA suggests using a footnote to clarify use of the term unaffiliated, such as “Use of the term unaffiliated is in relation to Black’s Law Disctionary defition for affiliated: ‘1. A corporation that is related to another corporation by shareholdings or other means of control; a subsidiary, parent, or sibling corporation. 2. One who controls, is controlled by, or is under common control with an issuer of a security.’”PROPER QUALIFICATIONS FOR RISK ASSESSMENT VERIFICATIONFMPA appreciates the challenges of defining qualification for independent verifiers while offering registered entities a broad choice for selection. We interpret that

Organization	Yes or No	Question 2 Comment
		requirements R2 and R6 grant the applicable entity sole authority to choose the 3rd party verifier as long as they meet the qualifications contained within those requirements. Is FMPA correct in that interpretation?CHANGE MANAGEMENT OF THE RISK ASSESSMENTThe standard is somewhat ambiguous on what happens if the responsible entity chooses to revise it's risk assessment of R1 sooner than the required 30 or 60 calendar months. Does every minor revision to the risk assessment require another 3rd party review? Or would only major system changes (e.g., due to adding a major new investment in the power system like a new 500 kV line) require review? Or regardless of system changes, would the review occur once every 30/60 months? FMPA suggests clarification to R2 to say that minor revisions to the risk assessment due to minor power system changes in between the 30/60 month periods do not need a separate 3rd party verification.
Georgia System Operations Corporation	No	GSOC supports the comments submitted by both Georgia Transmission Corporation (GTC) and NRECA
Georgia Transmission Corporation	No	-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.-GTC is concerned that the language of the standard and rationale around the use of the term "unaffiliated" in R
Hydro QuÃ©bec TransÃ‰nergie	No	Hydro-Quebec TransEnergie (HQT) agrees with this approach but requests that the SDT remove the term "unaffiliated" from Requirements R2 and R6.1HQT notes that the term "unaffiliated" is not used in FERC Order 146. Paragraph 11 of the Order states "In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator." Moreover, it appears that it is not FERC's intent to introduce this restriction regarding the choice of a third party. HQT therefore believes that the use of the term "unaffiliated" goes above and beyond what was stipulated in the FERC Order.Furthermore, the term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities (RC, PC and TP) that the SDT is seeking in the draft standard. The Reliability Model uses the term

Organization	Yes or No	Question 2 Comment
		"functional entity" to apply to a class of entities without making reference to specific organizations that register as functional entities.For some Canadian jurisdictions, the use of the term "unaffiliated" renders the standard more stringent due to the fact that certain Canadian entities such as Hydro-QuÃ©bec TransÃ‰nergie are simultaneously registered as TO, TOP, PC and RC. For integrated modeled entities, the restriction of available options that would otherwise be available (such as selecting a PC, TP or RC for the risk assessment verification under R2), makes it difficult to identify an entity with the required expertise capable of performing the reviews stipulated in the standard. HQT believes that the risk assessment of a TO should only be verified by the RC or the PC that has supervision (real-time or planning) over the said TO's assets because only the RC or the PC can ensure a comprehensive approach to critical facility identification that considers the reliability of an entire area.For these reasons, HQT believes that the expression "third party" alone is sufficient and consistent with the expressed concerns in the FERC Order.
Rayburn Country Electric Cooperative	No	I agree with the risk assessment in concept, the standard has far too many requirements and sub requirements to accomplish the task. Since initial analysis apparently this has already been done for the "High Risk" stations, a more efficient approach would be for the RC to perform the analysis based on the criteria mentioned to validate findings and find any second contingency facilities that may not have been identified. Since the RC is the "Reliability Coordinator", this is your third party identifying facilities without bias... Determinations will be based on an engineering basis utilizing standard uniform criteria across North America.The same analysis occurs for all entities within all regions, no variations this would yield consistency! Then the RC notify the entities that they have facilities that have been identified. (much like other NERC standards)Thus the information on which facilities have been identified would disseminated and controlled in a much more secure and better controlled environment while still maintaining the quality and consistency of the study needed.

Organization	Yes or No	Question 2 Comment
New Brunswick Power Corporation	No	In general, a TO may not have the capability to conduct a risk assessment to determine if an identified facility that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Such an assessment requires a wide area view of the Interconnection. It is proposed that the risk assessment be conducted by a PC, or RC for the area in which the facility is located. Doing so would satisfy the third party verification requirement as the TO would not be conducting the analysis. It is the opinion of NB Power that the technical details concerning the transmission analysis, in the proposed standard, are overly vague. This could lead to an inconsistent application of the analysis between entities as well as create obstacles with consensus concerning the proposed 3rd party verification. NB Power suggests a clear analysis methodology be drafted to establish a common basis for study criteria with the ability for each entity to apply additional specific requirements for their respective area.For corporate bodies, such as a vertically integrated utilities, that are registered as the RC, TOP, PC, TP and TO for a particular area, it is the opinion of NB Power that the requirement for unaffiliated 3rd party verification is overly stringent and of little value. The verifying party is limited to entities that have transmission planning or analyses experience, or, are registered as a PC, TP, or, RC from an adjacent area. NB Power is of the view that there are no unaffiliated entities with sufficient knowledge of the local transmission system to provide a meaningful verification within a 90 day period.As a government owned utility, NB Power is required to follow procurement processes which will make it difficult to meet the 90 day period for the third party verification. NB Power is also concerned that it could be non-compliant with the requirement if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance.It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated verifying 3rd party in requirement R2.3. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated verifying 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity

Organization	Yes or No	Question 2 Comment
		and an auditor may not be able to come to consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd parties recommendations.
Kansas City Power & Light	No	In R1, we have concerns about the ambiguity associated with the term "assessments". Can you provide examples of the types of assessments that would be acceptable to meet R1 and that would be CIP audit worthy in the future. We have the same concern in R2 with the term "third-party". Will there be a list of pre-approved third party contractors or will the RE's review and approve a third-party at the request of the registered entity prior to their use in the verification process as described in R2?
Central Hudson Gas & Electric Corporation	No	In regards to R2.2 as currently drafted, the unaffiliated verifying entity should have to ensure verification within 90 days and not the TO, since it is that entity performing the verification.In regards to R2.3 as currently drafted, there appears to be a lack of an appeals process in cases of disagreement between the unaffiliated verifying entity and the TO concerning the recommendations formulated by the unaffiliated verifying entity.
ITC	No	ITC believes that limiting physical security requirements in CIP-014-1 to those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection does not adequately raise the bar for critical infrastructure protection of valuable and strategic substation assets. Indeed, those substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection certainly warrant additional physical protection. However, so does any other substation asset deemed critical through the cybersecurity initiatives already in place through applicable companion Reliability Standards. If a substation is deemed critical through the CIP-002-5 screening process, it at a minimum, should warrant an “evaluation of potential threats and vulnerabilities of a physical attack to the facilities (CIP-014-1 R4). ITC supports using the brightline test criteria of CIP-002-5, as noted in

Organization	Yes or No	Question 2 Comment
		our comments for Question 1, above, but also feels that all substation assets passing the brightline test criteria should move directly to R4 for an assessment of threats and vulnerabilities, eliminating the need for R1 and R2. This has the benefit of using industry-vetted, bright-line criteria that creates valuable consistency between physical and cybersecurity assessment practices. This does not undermine the Commission's three-part requirement for addressing physical security, but rather allows the responsible entity to meet the Commission's first requirement (identification of critical assets) by using the same critical asset identification criteria for physical and cybersecurity. ITC believes if a facility is critical enough to warrant cybersecurity protection, then it should also warrant physical security and that the requirements should not be so narrowly defined to ignore the importance of substations beyond those few whose individual loss causes cascading outages. This simplified approach avoids potential contradictory and duplicative requirements between existing CIP standards, and would allow this standard to focus exclusively on physical security aspects and not on asset identification
Los Angeles Department of Water and Power (LADWP)	No	LADWP requests the Drafting Team to make the following changes:- For R1, additional time is needed to make sure studies are fully completed and reviewed by TO and its applicable governing authorities. Add ", which is due 30 calendar days after the effective date of the standard" to R1 as follows:"R1. Each Transmission Owner shall perform an initial risk assessment, which is due 30 calendar days after the effective date of the standard and subsequent risk assessments of its Transmission stations and Transmission substations (existing and....."- For R1, change "24 months" to " 30 months" to align the assessment with subsequent risk assessments.- For R2.1, The term "unaffiliated" needs to be defined in the standard to avoid any misinterpretation. - For R2.2, change the "90 calendar days" to "120 calendar days" to allow sufficient time to resolve differences if Planning Coordinator, Transmission Planner or Reliability Coordinator are addressing other deadlines.
Dominion	No	Measure M1 - R1.2 -- Measure M1 does not address sub-requirement R1.2 which requires the Transmission Owner to identify the primary control center that

Organization	Yes or No	Question 2 Comment
		operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment. Dominion recommends the SDT determine whether M1 should include the control center.R2.3 - Relative to R2.3, Dominion does not agree that the TO should have to document the technical basis for retaining assets that have been suggested for removal by the third party.R3 - Dominion suggests R3 be revised to strike the words 'and verified according to Requirement R2', and changing R2 to R1.2 in the next two instances where R2 is mentioned. This is due to the reason there is nothing included in R2 that requires verifing primary control centers.
MISO	No	MISO recognizes that the Commission mandated third-party verification of the risk assessment required under R1, however the current language of R2 requires modification to address several concerns MISO has with regard to its potential role as a verifying entity. While MISO has every confidence that it can perform risk assessment verifications in a safe, responsible, and accurate manner, the combination of a high number of requests requiring verification within a relatively short period of time presents some concerns to MISO regarding its resource allocation and availability. In particular, MISO recommends that the SDT add language limiting the universe of Transmission Owners/Operators that can seek verification from a particular verifying entity (potentially by geographical region or contractual or functional relationship) as well as modify the 90 day requirement to take into account that a single entity may have more requests than it can feasibly complete in such a short time period. An example of language that MISO could support is language that would allow a verifying entity and the requesting Transmission Owners/Operators to agree upon an appropriate completion date beyond the 90 days where the 90 day period will not allow completion of a robust verification due to resource constraints by the berifying entity. Finally, MISO respectfully requests that the SDT consider adding language to Requirement R2 that would allow verifying entities to limit liability related to both enforcement actions within the jurisdiction of FERC, NERC, and the Regional Entities and other actions that could be brought against verifying entities in other jurisdictions and venues unless it is shown that the entity lacked good faith or was grossly negligent.

Organization	Yes or No	Question 2 Comment
Omaha Public Power District	No	OPPD, in general, is in agreement with the approach taken in CIP-014-1 for identifying critical Transmssion stations and substations. We agree that risk assessment be conducted using transmission planning analysis, however, we suggest that this standard identifies what applicable planning analysis is used. We think the TPL standards provide the ability for the Transmission Owners to determine the worst case extreme event for identifying critical transmission stations and substations. OPPD believes that leaving R1 open and vague would encourage various interpretations of the term 'transmission planning analysis' as it applies to a 'risk assessment'. This may place the industry and the ERO in the same position as they were with the ealier versions of CIP-002 and the associated RBAM. Referencing the applicable TPL standards attemptes to remove some of this ambiguity by providing a more concise framework to evaluate those worst case extreme events. Furthermore, since TPL standards associated transmission planning analyses are performed in coordination with the PCs, risk assessment verification by PCs/RCs will not require a re-assessment of a study that has already been performed. We suggest that the SDT consider specifically defining 'transmission planning analysis' to avoid repeat of the uncertainty and vagueness associated with the CIP-002 RBAM. OPPD asks the SDT to consider revising requirement R1 as following: R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The transmission planning analysis shall be based on the applicable portion(s) of the TPL standards and specifically referenced. [VRF: High; Time-Horizon: Long-term Planning]1.1. Subsequent risk assessments shall be performed: o At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered

Organization	Yes or No	Question 2 Comment
		inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or o At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. 1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.
Ciy of Garland	No	R1 - The auditors should be limited to verifying that a study was completed using the assumptions agreed to by both the TO and the reviewer. The auditor should accept any study and assumptions jointly agreed to by the TO and the reviewer without requiring additional engineering justifications as to why one type of study was used instead of the auditor's preferred methodology. To summarize and echo FERC Commissioner Norris in his clarifying statement, included with the FERC Order that is the basis of the CIP-014 Standard, that if the Planning Studies indicate a transmission solution that would cause the substation to no longer cause the cascading outage that the transmission project could be initiated in lieu of the security plan. The additional transmission solution would potentially add other operational benefits other than just "security" and therefore may be more practical than the security plan in R4 through R6. In the guidance document, statements should be made that a TO may make additional planning studies at any time prior to the 30 months and if the third party reviewer concurs the updated study no longer shows a cascading event, whether due to changing grid conditions or system improvements, the standard would no longer apply including the continued implementation of the security plan. The TO should also notify the owner of the primary control center the substation no longer causes a cascading event.R2 - Timelines to complete third party verification under R2.2 and third party review under R6.2 are both too short. Increase 90 days to 120 days or 180 days. a. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES

Organization	Yes or No	Question 2 Comment
		Elements in adjacent Transmission Owner footprints. A 90-day time limit may not provide sufficient time to conduct and verify a revised or supplemental BES assessment.b. For security reviews, conducting an accurate and meaningful review with sound recommendations applicable to a specific TPs facts and circumstances may require additional time for assessment and discussions with the TO. A short review window is more likely to lead to misunderstandings, or disagreements with the TO which in turn could lead to discrepancies or improper application of the assessment requiring justification. This could cause the reviewer to avoid making recommendations that should be considered by the TO and improve the TO's assessment.c. As currently written, it appears if the TO disagrees with the reviewer's comments and writes a technical reason why he believes the original conclusion were correct, the recommendation(s) by the reviewer may be rejected and the TO's decision is final. Although I agree with this position it may be interpreted differently by the auditors. Please clarify which was the intent of the SDT.R3 - No comments
Bonneville Power Administration	No	R1 Terminology: Although the term "risk assessment" in this section is in alignment with language in the FERC order, BPA recommends that it be revised to consequence or impact assessment. This is a physical security standard, and the term risk assessment should be reserved for the physical security risk section of this standard and align with security industry use of the term. BPA believes the basic intent of R1 is to identify substation facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection can create unacceptable consequences to the BES and not to assess risk of the event happening.Also, BPA suggests that additional sub-requirements be added to provide clarity on what system conditions and performance criteria or methodology need to be considered in order to determine what stations and substations will be deemed critical. Similar language found in existing standards would be helpful. Examples: FAC-010-2.1 (System Operating Limits Methodology for the Planning Horizon), R1-R3; FAC-013-2 (Assessment of Transfer Capability in the Near-Term Planning Horizon), R1; TPL-001-4 (Transmission System Planning Performance Requirements), R1-R6; TPL-004-0a (System Performance Following Extreme BES Events), R1."R1 1.1. Subsequent risk

Organization	Yes or No	Question 2 Comment
		assessments shall be performed:" BPA recommends revising R1 1.1 to: “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.” Justification: This would consolidate the two bulleted actions and make them equally applicable. BPA has been doing substation facility impact and security risk assessments for the past 15 years and our experience is that the criticality of a substation facility does not change once ranked; once it is determined critical it will always be critical particularly when information is used in a physical security risk assessment. A 5 year interval would be a more appropriate interval for this type of assessment as it would always be case of identifying new facilities and not excluding ones previously identified."R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. [VRF: Medium; Time-Horizon: Long-term Planning]"BPA recommends revising R2 first sentence to: "R2 Each Transmission Owner shall verify the impact assessment performed under requirement R1 by a third party entity other than the owner or operator." Justification: This fully aligns with the requirements of the FERC order by using the requirements of the FERC order. BPA believes the introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of an impact assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes that the word unaffiliated be removed from this standard and replaced with language that describes the degree of separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft “unaffiliated” is especially troublesome for federal government-owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the federal government transmission owner.Also, BPA believes industry peer reviews should be

Organization	Yes or No	Question 2 Comment
		encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into widespread use. Please note that the FERC order only recommends this verification as it is stated as “should” and not as “shall.”"R.3 For a primary control center(s) identified by the Transmission Owner according to Requirement R1 and verified according to Requirement R2 that is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. [VRF: Lower; Time-Horizon: Long-term Planning]" BPA recommends revising the 7 day requirement in R3 and R3 3.1 to 30 calendar days. Justification: This information is not that time critical at this stage, and one week will not be enough time to complete all notifications.
National Rural Electric Cooperative Association (NRECA)	No	R1.1 - NRECA recommends that the 30 months timeframe be revised to 36 months as an annual focus is more straightforward than a 2.5 year focus and it’s easier to track for internal programs and controls. 60 months should also be increased to 72 months to maintain the double timeframe that currently exists in the draft requirement.R2 - The March 7 FERC order does not require an owner or operator to select an entity to verify its critical facilities assessment. The order uses the word “should,” not “shall” or “require.” The rationale for R2 is not accurate in this sense and should be revised to match the language in the order. Additional clarity is needed regarding what “verify” means in the standard. Guidance and rationale is helpful, but does not carry to legal weight of the standard language. R2.1 - This section should explicitly include NERC and the Regional Entity (RE) as a potential verifying entity. NERC and the RE should be obligated to perform this role if the owner or operator requests them to do so under this standard. There should not be a direct or indirect requirement to mandate the registered entity to hire a third party to verify the assessment portion of the standard. If a registered entity wants to hire a third party, that should be a decision the

Organization	Yes or No	Question 2 Comment
		registered entity makes, but is not required for standard compliance. If a third party, other than NERC or the RE, verification of the assessment is required by the standard, then this is effectively two audits on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted. Are there enough non-NERC/RE third parties available for what is likely to be a high demand for services, especially if there's a short time period as currently drafted? This is similar to the shortage of vendors that industry faced in the NERC facility ratings alert responses. How is "transmission planning or analysis experience" judged by NERC compliance and enforcement? This language could be very difficult to comply with depending on the purview of the auditor. If a registered entity hires a third party to develop and complete an assessement as required in the standard, can that third party also verify the registered entity's assessment? As drafted, the current standard could be read to require two third party entities to be hired - this would be unreasonable and the standard should be revised to clarify that only one third party would be needed to comply with the standard.R2.2 - This requirement appears to require the third party entity to comply with language in the requirement. This does not seem to be appropriate or legal. The drafting team should revise the language to redirect the compliance burden to the NERC registered entity. In addition, the 90 day requirement could be difficult to comply with if there is a shortage of third party entities to contract with. Consideration should be given to revising this requirement to prevent a registered entity being found in violation of a requirement due to circumstances not under its control. R2.4 - The words "exchanged with" should be changed to "made available to" in order to clarify that information may not be exchanged, but rather presented for viewing only, to a third party entityR3.1 - The 7 day requirement appears to be unnecessarily short and not immediately necessary for BES reliability. NRECA believes 30 days is more appropriate timeframe for this requirement.
PNM Resources	No	R2.1 could place an unreasonable burden on entities registered as PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed

Organization	Yes or No	Question 2 Comment
		in 90 calendar days on the TO. As a TO an entity cannot compel another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
PNM Resources	No	R2.1 puts an unreasonable burden on registered PC and TP. R2.2 which puts the burden of ensuring that the unaffiliated third party review is completed in 90 calendar days on the TO. As a TO PNM can't force another registered entity or third party to complete anything with a specified amount of time and according to the RSAW if the verification is not completed within 90 days then the TO is not in compliance with the requirement. The standard should require registered NERC entities to complete the unaffiliated review and those entities should be included as applicable functional entities and R2.2 should apply to the reviewing entity.
Tri-State Generation and Transmission Association, Inc.	No	Rather than making it the Responsible Entity's responsibility to find a third party to verify its assessment, Tri-State believes it would better suit the industry and the standard if R2 required either the Reliability Coordinator or Regional Entity to request TO's assessments on an intervaled basis. This meets the requirements of the March 7 FERC Order. Allowing the requirement to be broad enough to allow third party paid consultants with "transmission planning or analysis experience" creates a conflict of interest and contradicts the draft standard's requirements for the use of "unaffiliated third part[ies]". If third party - other than NERC or the RE - verification of the assessment is required by the standard, then this is effectively two audits (and two 3rd party assessments) on the same requirement. Additionally, it does not seem appropriate (or potentially even legal) for a third party (other than NERC or RE) to be able to add or remove facilities from a critical facilities list as the standard is currently drafted.Tri-State recommends that rather than 30 months and 60 month risk assessment intervals for R1.1, they should be a more straightforward 36 months and 72

Organization	Yes or No	Question 2 Comment
		months respectfully in order to be consistent withnormal auditing time periods of three years. This will make the intervals easier to track with internal programs and controls.
Bureau of Reclamation	No	Reclamation agrees with this approach. However, to promote consistent identification of critical facilities within an interconnection, Reclamation believes that the third-party review should be conducted by the Transmission Owner (TO)'s Planning Coordinator or Transmission Planner. If the Transmission Owner is also the Transmission Planner and Planning Coordinator, the third-party review should be performed by the Reliability Coordinator. Reclamation also suggests that the drafting team modify the term "risk assessment" to "BES impact assessment." In the physical security community, the term "risk assessment" generally refers to "The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel." See ASIS International, General Security Risk Assesment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC can explain that it adopted the term "BES impact assessment" so it is clear that the initial evaluation is of risk to the BES if the substation is rendered inoperable or damaged. Reclamation also recommends revising R1.1 to require subsequent risk assessments every 60 months for all Transmission Owners. Reclamation believes that periodic risk assessments are necessary, but has not seen evidence that the costs associated with updating risk assessments every 30 months rather than every 60 months would provide commensurate reliability benefits. Reclamation recommends that the drafting team update R1.1 to state, "Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment."
SERC CIPC	No	Recommend that the Transmission Planner perform the risk assessment in R1 instead of the Transmission Owner. Need further clarification and examples for the term "unaffiliated". Would "peer" reviews studies that do not have a single registered entity with controlling interest suffice as an "unaffiliated" third party reviewer? What role

Organization	Yes or No	Question 2 Comment
		does the SDT envision the ERO (including regional entities) playing in the review process?
Foundation for Resilient Societies	No	Same answer as provided to Question 1.
Southern California Edison Company	No	SCE has concerns with both Requirement R1 and Requirement R3. In Requirement R1, SCE recommends that the verbiage be changed from “...that if rendered inoperable or damaged could result in widespread instability...” to “...that if damaged to the point of being rendered inoperable could result in widespread instability..." SCE requests this change to reduce ambiguity in the application of the word "damaged." In addition, language should be added to R1 that specifies: “...system instability such as uncontrolled separation or cascading within 15 minutes of compromise...,” as a 15-minute window would align with criteria in the CIP standards used to determine critical facilities. In the guidance section for R1, SCE would suggest changing the text from “...remedial action schemes (RAS) or special protection systems (SPS)” to “...special protection systems (SPS)...,” because as used in the NERC Glossary of Terms, a RAS is included as a type of SPS. In addition, SCE requests that R1 be revised to include specific examples and criteria for the risks to be measured. For instance, SCE believes the following could be among the examples and criteria specifically included: (a) Thermal overloads beyond facility emergency ratings; (b) Voltage deviation exceeding Â± 10%; (c) Cascading outage/Voltage collapse; and (d) Frequency below under-frequency load shed points.With respect to Requirement R3, SCE requests that additional guidance be provided on how a "primary control center" should be identified, as that term in used in both Requirements R1.2 and R3. SCE also asks the team to consider changing the notification requirement in R3 from seven(7) to thirty(30) days in order to allow sufficient time for the transmission owner and transmission operator to perform the required communication.

Organization	Yes or No	Question 2 Comment
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	No	Specifically, Vectren recommends that R2 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to designate registered Planning Coordinators, Transmission Planners, or Reliability Coordinators as the approved verifiers for entity risk assessments AND to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered "qualified" by FERC, NERC or NERC auditors who might review the results later - leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity's selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.
Southwest Power Pool Regional Entity	No	SPPRE believes that greater clarity is required with respect to the risk assessment to be performed. At a minimum an extreme contingency study needs to be performed that takes out the entire facility, all voltages present. The study should also not consider any operating guides or other mitigation when evaluating the impact of the outage. In Section 2.3 technical basis should be changed to engineering basis. Additionally, the unaffliated verifying entity should not be the party performing the original study, under the principle that an auditor cannot audit ones own work; to do so would not be consistent with the expectation of verification by an unaffiliated entity.

Organization	Yes or No	Question 2 Comment
Salt River Project	No	SRP supports comments submitted by APPA with the following additions:The time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. If possible, could the drafting team revise the language of Requirement R1 to make this clear?The periodicity of the risk assessments required by Requirement 1 and the time frame that the risk assessments appear to not align. The risk assessment is required to include Transmission stations and Transmission substations that exist as well as those planned to be in service within 24 months. However, the periodicity for conducting future risk assessments is every 30 calendar months or every 60 calendar months if the prior risk assessment did not identify any Transmission stations or Transmission substations. This potentially leaves a gap of six to 36 months where facilities may not have been assessed.In R2 it is not clear that the primary control center must also be verified, but in subsequent requirements it implies or states that it should be. If the intent in R2 is that the primary control center should also be verified, then it should state so in R2.2 and R2.3 in addition to stating stations and substations.Third Party Verifiers:SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered

Organization	Yes or No	Question 2 Comment
		Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities.Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers.Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.

Organization	Yes or No	Question 2 Comment
FortisBC	No	The audit provides an independent review of an entity's application of the standard and therefore, an additional third party review should not be required as described in R2.It is agreed that if a null set is identifed, the rest of the standard does not apply.
Western Electricity Coordinating Council	No	The periodicity for risk assessments and the forward looking time frame for including planned substations do not match. Entities are only required to consider stations planned in the next 24 months, while the risk assessment is applied on a 30 month cycle, or a 60 month cycle if the entity previously identified a null list of applicable stations. This potentially leaves a 6 to 36 month gap. We would encourage the SDT to match the periodicity of the application to the planned implementation window or include language requiring any new asset be evaluated under R1.WECC notes that the time frame for completion of the initial risk assessment required in Requirement R1 is not identified in the standard, only in the implementation plan. This may be a point of confusion for entities that fail to fully read and understand the implementation plan. WECC suggests that at a minimum NERC and the Regions engage in extensive outreach to ensure that the Transmission Owners are aware of this and that if possible the drafting team revise the language of Requirement R1 to make this clear.Requirement R2, part 2.2 appears to be assigning responsibilities to the unaffiliated verifying entity (registered Planning Coordinator, Transmission Planner, or Reliability Coordinator) yet these entities are not included in the applicability section. If these entities are to be held accountable in the standard for actions, why are they not included in the applicability section?
Northeast Power Coordinating Council	No	The Rationale Box for Requirement R2 stipulates that "'unaffiliated' means that the selected verifying entity cannot be a corporate affiliate (i.e., the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission o(O)wner)." This conflicts with Requirement R2 Part 2.1 which lists "A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or An entity that has transmission planning or analysis experience" as those qualifications for an unaffiliated verifying entity. Clarification is needed that an Independent System

Organization	Yes or No	Question 2 Comment
		Operator that has operating authority over an entity is eligible to be the unaffiliated verifying entity.
None	No	The SDT has not factored in the resiliency concerns stated in the FERC order. Many of the facilities selected by the initial screening process will have long lead time equipment that if damaged will be out of service for several months. The assessment process needs to consider the operational risks during the time that the TO is waiting for replacement equipment. R1 should be amended to include the following sub-requirement.If the facility being studied has long lead time items, i.e. 4 months or greater, the study must include an N-1 analysis for the widespread instability, uncontrolled separation, or Cascading within an Interconnection test.In addition, the premise for this standard is a physical attack resulting in faulted equipment. There is no mention of the assessment being conducted for the Facilities under fault conditions and in many cases under delayed clearing.R1 should be amended to include the following sub-requirement.The analysis of the subject Facility must include dynamic simulation of faulted conditions with delay cleared for the most severe contingency within the Facility.The phrase "instability, uncontrolled separation, or Cascading" is core to the definition of Interconnected Reliability Operating Limit (IROL). Every RC and PC has an IROL methodology under the FAC standards. R1 should be amended to include the following sub-requirement.The test for instability, uncontrolled separation, or Cascading must be consistent with the IROL methodology established by PCs and RCs under FAC-010 and FAC-011.
SPP Standards Review Group	No	The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. “These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken

Organization	Yes or No	Question 2 Comment
		individually, one at a time." While not specifically referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments. We strongly suggest that the SDT expand on this addition to R1 in the guidance document to provide needed clarification to the industry.
Westar Energy	No	The Standard intentionally does not provide specific methodologies regarding the type of analyses needed to be conducted for the assessments in R1. This leaves the door open to very different interpretations across the industry. We suggest the drafting team consider specifying analyses such as those contained in the TPL standards. This would eliminate confusion within the industry and provide clear direction for those conducting the analyses. We suggest adding the following sentence at the end of R1. "These analyses will include consideration of the entire loss of the Transmission stations and Transmission substations specified in Applicability Section 4.1.1 taken individually, one at a time." While not specifically referencing the TPL standards (currently enforceable TPL-004-0a, R1 and TPL-001-4, R3 to be enforced in 2016) which cover the loss of switching stations and substations, this language provides guidance regarding the type of analyses to be conducted in the assessments.
Nebraska Public Power District	No	The third party verification is unnecessary and should be deleted from the standard. There is no other unaffiliated third party that has knowledge and expertise comparable with the incumbent Transmission Planner who develops the detailed models, performs the reliability assessments, and develops the required long term plans for the Transmission Owner on an annual basis. If the verification remains in the standard, 90 calendar days is not a sufficient amount of time to complete verification. A Transmission Planner may ask a Planning Authority (PA) to review its risk assessments, but the same PA will likely be asked to review multiple utilities. Recommend at least 180 days to complete the verification.

Organization	Yes or No	Question 2 Comment
Encari	No	There should be a strong, rebuttable presumption that an applicable Transmission Facility requires physical protection owing to its classification under the bright-line "medium impact" rating criteria under CIP-002-5.1 (which is repeated in the Applicability section of CIP-014-1 for Transmission Facilities). The utility of a risk assessment could be recognized, however, as justification for rebutting the presumed need for a set of mandated physical security measures.
Consumers Energy Company	No	We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
Cooper Compliance Corp	No	We do not support the Standard as written today. We agree with the scope and content of the SAR. However, we are concerned with Requirement 6. Requirement 6 requires entities to seek out third parties to review their new physical security protection plans. We don't believe that entities should be obligated to seek assistance from third party individuals. This includes consultants or another unassociated entity. The purpose of the regions, NERC, and FERC are to provide a review of an entities compliance to Standards through the audit and self-certification process. No other Reliability Standards require an entity to use third parties to determine compliance or sufficiency of compliance documentation. We believe that this obligation may place some entities in difficult financial situation and could have a negative impacts in assuring that proper third party entities are being used. Should FERC, NERC, or WECC determine that entities are not following the spirit of the Standard than they may request a modification in a future Standard revision. We will support this Standard if Requirement 6 is removed.
Independent Electricity System Operator	No	While the proposed R1 to R3 collectively meet the FERC requirements for having an entity to identify the critical facilities and having the assessments of such identification verified, we believe it is more appropriate that the 3rd party verification be performed by NERC registered entities only (which could be the Reliability Coordinator, Planning

Organization	Yes or No	Question 2 Comment
		Coordinator or Transmission Planner). An entity that has transmission planning or analysis experience may only have an outside equivalent representation of the BES and their ability to conduct an analysis with a "wide area" view of consequences may not be possible. As such, we suggest to revise Requirement 2.1 by eliminating the second bullet point : "An entity that has transmission planning or analysis experience".
National Grid	No	While we support using the CIP-002-5.1 criteria as a starting point for applicability of the draft standard, we do have concerns with the inclusion of the phrase "within an Interconnection" in R1. FERC Order RD14-6 directs that "[a] critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System". By introducing the word "within," the Standard could inadvertently draw widely different interpretations of how to assess risks to the BPS. In practice, this could open up the potential for the inclusion of regional or localized transmission impacts, which we believe is in contrast with the Commission intended scope in the Order.As a result, we suggest that the wording in R1 be modified to the following:"A critical facility is one that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation or cascading failures widespread across significant portions of an Interconnection".Alternatively, we recommend clarifying in the guidance documents that 'widespread' and 'within an Interconnection' proposed words are intended to apply to impacts to the BPS that reaches deep into the Interconnection, and not affecting a small portion of an Interconnection. For example, if an Interconnection has relatively small Balancing Authorities (BAs), 'widespread' would need to be interpreted as impacts that would be crossing several, i.e. more than two, of those BAs in order to be considered 'widespread'.
Herb Schrayshuen	No	In Requirement R1 the use of the term 'transmission analysis' and 'transmission analyses' in order to identify which substations should have a security plan is vague The TPL standards extreme cases should be used to clearly describe the specific required elements of the analysis. Failure to specify how the analysis is to be done will lead to inconsistencies in the analysis and thereby difficulty for audits of the standard.

Organization	Yes or No	Question 2 Comment
		In Requirement R2 the use of the word 'unaffiliated' introduces ambiguity. There needs to be an understanding (through the standard but if not feasible through RSAW or other tool-e.g. guideline) what "unaffiliated" means. The term "unaffiliated" is not required because the NERC Reliability Functional model already ensures the independence between the TO/TOP and the verifying entities.
ATCO Electric	Yes	Although the FERC order contains language that a third party verification occur, this type of verification is not used anywhere else in NERC reliability standards for similar activities (e.g. CIP-002 classification). ATCO Electric (AET)respectfully requests that the review be allowed to be performed by qualified in-house Engineering groups who already perform these functions. Mandating a third party verification presents a risk to timelines and the implementation of the other requirements.
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.TIMELINES to complete third party verification under R2 and third part review under R6 are both too short. Increase 90 days to 120 days or 180 days. Verifying entities may recommend that the Transmission Owner conduct additional planning studies to confirm asset identifications such as interactions between BES Elements in adjacent Transmission Owner footprints. A short 90-day time limit may not be sufficient time to conduct and verify a revised or supplemental BES assessment. For security reviews, conducting a meaningful review with sound recommendations applicable to a specific TO's or TOP's facts and circumstances may also take time along with necessary discussions with the TO. A short review window is more likely to lead to disagreements with the TO which in turn would lead to discrepancies that would need to be justified - which in turn might cause the reviewer

Organization	Yes or No	Question 2 Comment
		to avoid making proposals that should be considered by the TO or pressure on the TO to accept recommendations that could be improved upon.R1 GUIDANCE - TRANSMISSION PLANNING BASE CASES: Please revise the Guidance for R1 to clarify that TOs should start their initial and subsequent risk assessments with a common regional or area transmission planning base case used for transmission planning purposes. The base case should include existing BES stations and substations and those planned to be in service within 24 months within the region or area, to ensure forward-looking risk assessments and security planning.R2 VERIFICATION - Third party verification of third party risk assessments conducted under R1: some medium sized TOs with applicable transmission stations and substations may contract with a third party consultant to conduct necessary BES risk assessments, to ensure accurate and comprehensive consideration of the risk of widespread cascading, instability and uncontrolled separation. Such entities seek clarification that a single expert risk assessment study, in conjunction with a verification by an unaffiliated PC, TP or RC would suffice.
Arizona Public Service Company	Yes	AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications for Requirements 1-3.AZPS suggests that the drafting team modify the term “risk assessment” to “BES impact assessment” in Requirements 1-3. The term risk assessment is not a defined term in the NERC Glossary of Terms. It is used in other CIP standards (CIP-002, and CIP-004) each with a different context. Changing the term to “BES impact assessment” ensures that the risks will be categorized and evaluated correctly.Requirement 2.1 directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment. However, none of these NERC functional entity designations appear in the applicability section of the standard. Thus it is assumed that the entities listed above are not obligated to conduct the assessment once selected but rather the assessment is conducted by mutual agreement. AZPS suggests that the drafting team provide clarifying language in the requirement to indicate that the assessment is conducted by mutual agreement between the Transmission Owner and the third-party assessor.AZPS is concerned that the term “primary control center” will

Organization	Yes or No	Question 2 Comment
		be confused with the NERC Glossary Term “Control Center.” The definition of Control Center is partially defined as “monitor and control the BES...”. The rationale for Requirement 1 introduces the term “operationally control” in its definition of primary control center which is further defined to mean “causing direct physical action”. The concept of monitoring is explicitly excluded from this definition. To avoid confusion, AZPS suggests that the drafting team define the term primary control center or adopt a new term that clearly differentiates itself from the common term “control center”.
FirstEnergy	Yes	FirstEnergy supports the proposed requirements R1 through R3.
Idaho Power Co.	Yes	Further clarification is needed on several points. There is no specificity to provide consistency with how the "risk assessment" should be performed or what methodology or components to the methodology should be used. Additionally, there is no defined meaning of "widespread instability, uncontrolled separation, or Cascading within an Interconnection." Does this refer to regionally identified IROLs or some other objective criteria or only based on the analysis performed? Additionally, there is no mechanism built into R3 to allow for a dispute between a TO and a TOP if they disagree on a particular station or substation as there is in the third party reviews under R2 and R6 where there is a mechanism to disagree with the reviewer.
Public Utitliy District No. 1 of Cowlitz County, WA	Yes	However, the TOP does not receive any relief from R1-R2 null set(s) and will be required to provide attestations to auditors and yearly certification of the absence of any notice from Transmission Owners.
MidAmerican Energy Holding Company	Yes	MEHC agrees with the R1 through R3 approach. However, MEHC suggests the following changes to improve the standards as written:The term “unafilliated third party” is used in R2 and in R6, but in parts 2.1, 2.3 and 2.3. “unaffiliated verifying entity” and in part 6.3 “unaffiliated reviewing entity” is used. Unless the intent was that the terms have different meanins, it is suggested that “unafilliated third party” be used throughout the standard.

Organization	Yes or No	Question 2 Comment
NRG Energy, Inc.	Yes	NRG agrees the approach described in Requirements 1 through 3 address the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: o Primary control centers are referenced in the "purpose" of the standard, but are not included in the "applicability" section. For clarity, NRG suggests the addition of section 4.1.1.5, stating "Control Centers and backup Control Centers associated with the Transmission stations and Transmission substations identified in requirements 4.1.1.1 through 4.1.1.4." o R1 directs that the Transmission Owner to perform an initial risk assessment with subsequent studies and include an unaffiliated third party to verify the risk assessment performed. NRG is concerned the standard does not indicate how information shared under this Requirement will be protected and held in confidence. NRG believes the information subject to this standard should be treated as Critical Energy Infrastructure Information (CEII). o R1 is vague in providing guidance as to the criteria to be used in developing the risk assessment. NRG appreciates this is intentional to allow flexibility in developing the assessment. However, this results in the potential for a determination of non-compliance during the audit process. NRG suggests reliance on the CIP-002 standard used for defining Critical Assets, which is based on solid metrics. o R2 seems to allow the same third party to perform both the initial risk assessment and the review of the initial risk assessment, potentially negating the need for a separate review. o R2.2 calls for review of the results of the initial risk assessment by an unaffiliated third party. The standard provides no guidance regarding the criteria (assumptions, contingencies, etc.) to be used for this review, which could provide results differing from the initial assessment. More objective measures should be incorporated.
Xcel Energy	Yes	Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team.R1 requires an assessment of facilities, including those to be in service within the next 24 months, followed by an additional review every 30 or 60 months. If a facility is brought into service, it is unclear when the review should be performed due to the 6 month gap between the in service date and

Organization	Yes or No	Question 2 Comment
		the review. R2 requires a Transmission Owner to have an unaffiliated third party "verify" the risk assessment performed under R1. By contrast, R6 requires each Transmission Owner to have an unaffiliated entity "review" the evaluation performed under R4 and the security plan under R5. Xcel Energy recognizes that use of "verify" and "review" reflects the Commission's wording, but it would be helpful if the standard explained the difference between the two terms, if there is a difference.The 90 days prescribed by R2 to obtain third party verification may be too restrictive due to the availability and/or capacity of applicable resources. The standard requirement which imposes the action/deliverable by a third party, but the accountability to the TO/TOP, is also a cause for concern. It might be better to have the timing of R1 and R2 combined as this would enable flexibility of performing the assessment and completing the third party verification within the overall timeframe desired. We also suggest the Regional Entities or NERC be considered as parties that can provide third party verification and contract out if desired. It would also be helpful to expressly clarify in R2.1 that an "entity with transmission planning or analysis experience" could include a peer TO/TOP or a panel of employees from peer TO/TOPs, for example from the North American Transmission Forum. Allowing peer review would assist in identification and dissemination of best practices, we believe.R2.3 requires documentation of any recommendation to add or remove facilities as recommended by the verifying entity, but does not specify if any actions are required if no recommendations are made. Since the VRFs reference various levels of severity based upon documentation of recommendations, it would seem beneficial to allow a "no recommendations" option. Also, it is unclear if there are specific criteria the third party reviewer should utilize to review/verify and make recommendations if facilities are to be added or removed. While an entity could indicate why recommendations were or were not adopted, it would be useful to have verification criteria defined more clearly. R3 seems to be unclear in whether TOs or TOPs have operational control over facilities. In order to more clearly identify that TOPs have operational control, R3 should indicate that the TO shall notify the TOP of the identified facility.

Organization	Yes or No	Question 2 Comment
Peak Reliability	Yes	Peak believes the RC entity should perform the R2 verification because the RC has the wide-area view in the Western Interconnection. The alternative would be to have individual transmission entities perform varied verifications, which could result in inconsistent methodologies and results.
ISO/RTO Standards Review Committee	Yes	R1R1 in conjunctions with the Applicability section is a reasonable approach for identifying the scope of facilities subject to R2 - R6.R2Imposing a verification requirement is a reasonable way to facilitate an effective outcome in terms of identifying facilities that meet the impact thresholds established in R1. Requiring the use of an unaffiliated third party is reasonable because it mitigates the potential for inadvertent error in study work. Finally, allowing the verification to occur concurrently or subsequently, and leaving that decision to the discretion of the relevant functional entities, is appropriate. The functional entities should have the discretion to determine the most effective means of performing the verification. R2.1 requires that the verifying entity be either 1) a registered RC, PC or TP, or 2) another entity with appropriate planning or analysis experience. This is a reasonable approach that provides appropriate flexibility with respect to third party verification options. It also addresses the different operational and planning structures that comprise the North American electric grid - i.e. organized market regions where different entities can perform the different NERC registered functional roles (ISOs/RTOs) and vertically integrated regions where all the relevant roles under the standard may be performed by a single entity and, therefore, would require the use of an independent third party to perform the unaffiliated verification. R2.2 requires the third party verification to either confirm the TO analysis under R1, or, alternatively, recommend that facilities be added or deleted (the IRC assumes that a verification can confirm some results and also add facilties or remove facilities). Although R2.2 establishes a reasonable standard - i.e. verify TO results or recommend changes - the IRC offers the following comments. The requirement, as written, imposes the obligation on the third party verifying entity. However, the TO is the responsible entity under the standard - i.e. the TO is required to obtain the third party verification. The language should be revised to clarify that the

Organization	Yes or No	Question 2 Comment
		relevant actionable obligation (to obtain the third party verification) lies with the TO. The next issue raised by R2.2 is the timing. The IRC appreciates the importance of the issues being addressed by the proposed standard and the goal of implementing the standard and the relevant processes contained therein in a timely fashion. However, practically speaking, 90 days may be difficult to meet depending on the number of Transmission Owners that require verification from a single Registered Entity. For example, in organized markets there may be numerous TOs all selecting their PC to verify. To the extent implicated in reviews under the standard, IRC members would make best efforts to perform any relevant verifications. This comment is merely intended to highlight the potential resource impacts under the proposed 90 day timeline. The IRC proposes the following revisions to mitigate the issues in R2.2 described above. 2.2. The third party verification shall either verify the Transmission Owner's risk assessment performed under Requirement R1 or recommend the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within a mutually agreed upon timeframe between the Transmission Owner and the third party but no longer than 180 calendar days following the completion of the Requirement R1 risk assessment. R3R3 obligates the TO to notify a TOP that has operational control of a control center associated with a facility identified pursuant R1 and verified under R2. R3.1 requires similar notification if a facility is removed via those processes. The standard may benefit from including the draft guidance into the R3 rationale section that clarifies that operational control means the ability to take action that affects the physical status of the facility, and that it does not include directive control, which relies upon another entity to take operational action to change the status of the facility. The guidance document addresses this issue, but the SDT could add clarifying language to the rationale section of R3, similar to the language in the guidance document and/or the language in the R1 rationale section, which reads in relevant part:"... identify the primary control center that operationally controls that Transmission station or Transmission substation (i.e., the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the

Organization	Yes or No	Question 2 Comment
		ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).”
Pacific Gas and Electric Company	Yes	R2 Comment: Suggest removal of the requirement for a third party risk assessment verification. Verifications already occur as part of internal compliance programs in CIP-002 and when audited by the Region. What if the assessment is performed by a third party, do you have to get another third party to verify? This creates a significant administrative burden, even if the Standard will only apply to a small number of entities and facilities.R3 (pg. 8) “...the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify...” Comment: Seven calendar days may be too short a time requirement, consider 10-14 days
Basin Electric Power Cooperative (BEPC)	Yes	R2 - A concern to consider is whether there is an adequate pool of unaffiliated third party verifiers to meet the 90 day timeframe. Possible solutions would include (1) increase the 90 day requirement to six months; or (2) Revise the requirement to allow the NERC Registered Entity to notify the appropriate Regional Entity of the verifier pool constraint and request the Regional Entity act as the verifier or specify an acceptable alternative.
Public Utility District No. 2 of Grant County, WA	Yes	R2 references primary control center(s). Since Control Center is a NERC defined term GCPD suggests that all references to the Control Center be capitalized within the Standard and that “primary” be defined within the standard to not include “back-up” Control Center(s).
Exelon	Yes	R2.1 Drafting Team could consider adding a note to R2 Guidance section similar to that which is included in the recently approved MOD-032 standard.”Planning Authority and Planning Coordinator" (hereafter collectively referred to as “Planning Coordinator”)combines “Planning Authority” with “Planning Coordinator” in the list of applicable functional entities. The NERC Functional Model lists “Planning Coordinator” while the registration criteria lists “Planning Authority” and they are not yet

Organization	Yes or No	Question 2 Comment
		synchronized. Until that occurs, the proposed standard applies to both Planning Authority and Planning Coordinator."
ReliabilityFirst	Yes	ReliabilityFirst supplies the following comments for consideration:1.Requirement R1 - ReliabilityFirst believes there may be a gap in the timing of performing the risk assessment for new Transmission stations and Transmission substations which are planned outside the 24 month window as required in Requirement R1. For example, as written, if a new Transmission stations or Transmission substation is planned for month 25, it would not be included within the initial risk assessment. Thus, there is a potential for this new Transmission stations or Transmission substation to not be assessed for 30 calendar months (for a Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable ...) or 60 calendar months (for a Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability..." With the potential gap in assessing new Transmission stations and Transmission substations being so long, ReliabilityFirst believes reliability may be compromised. For these reasons, ReliabilityFirst recommends the following for consideration: "Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 30 months)..." and including a new bullet under Part 1.1 which states "At least prior to the implementation of all new Transmission stations and Transmission substations (if not assessed within the initial or subsequent risk assessment)"2. Requirement R3 part 3.1 - From a standards writing perspective, if there is only one sub-part, ReliabilityFirst recommends including it within the Parent requirement R3. Typically sub-parts are only included if there are more than one.
Northeast Utilities	Yes	Requirement 1 should match that language in the FERC order and not limit the assessment to Transmission System analysis and allow for an opportunity to apply

Organization	Yes or No	Question 2 Comment
		technical expertise and judgment prior to the Transmission System analysis. We agree to Requirement 2 and Requirement 3.
PPL NERC Registered Affiliates	Yes	Requirement 1: 1. Requiring completion of an initial risk assessment for Transmission stations and substations planned to be in service within 24 months can lead to audit difficulties. Planned in service dates often change for a variety of internal or external reasons. It is requested that the SDT consider changing this language to a more easily identifiable trigger such as requiring the risk assessment to be performed before a new Transmission station or substation is energized. 2. Does the R1 risk analysis require consideration of the impact of loss of lines with voltages below 200 kV in an identified Transmission station or substation? 3. It is unclear when the R.1 risk assessment needs to be completed. This should be clarified.4. The wording in the Rationale for Requirement 1 box identifies the primary control center, but it also notes that control center electronic actions can cause direct physical actions at the Transmission station and substation. This would typically implicate the backup control center as well because the backup control center will have similar functional capabilities. There appears to be a disconnect between the use of the term primary control center and the parenthetical that follows which appears to include any control center that performs the listed functions.
San Diego Gas & Electric	Yes	SDG&E agrees with this approach. A facility's identification as "medium impact" does not necessarily mean that the facility, if rendered inoperable or damaged could result in widespread instability, uncontrolled separation or Cascading within an Interconnection. Application of a risk assessment will ensure that CIP-014-1 is focused on the facilities that are most critical to the system.
Seattle City Light	Yes	Seattle City Light supports the Question 2 comments of APPA as well as the additional comments of Salt River Project (SRP) regarding 3rd party verification.Third Party Verifiers (SRP):SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in

Organization	Yes or No	Question 2 Comment
		regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance responsibilities.Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers.Confidentially of

Organization	Yes or No	Question 2 Comment
		the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
Seminole Electric Cooperative, Inc.	Yes	Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. As this standard is based on the same standards as the impact ratings in CIP-002, it would be cleaner to identify any facility that is determined critical under the Assessment with a separate (non-exclusive) impact rating such high physical impact and use this term for applicability for R3-R6. If an entity has a qualified third party perform the R1 assessment on behalf of or in cooperation with the registered entity, does this also meet the requirement R2? Note that the draft RSAW, not under review here, states that R1 and R2 may occur concurrently. R2.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to note that this information is included in the materials subject to enforcement under CIP-011-1 R1.
Vermont Transco LLC	Yes	Specifically the filtering of assets. While starting with CIP-002-5.1 as a starting point, the amount of analysis and assessment to determine if these facilities are critical and applicable to this standard may not be possible in the timeline proposed for this standard if a full transmission planning analysis will be needed. Many planning analysis performed previously by entities were not assessed to the specific defininition included in this requirement and therefore could require considerable work to be performed to analyze. The wording suggests that a full transmission planning assessment should be performed for all CIP-002-5.1 facilities and not to just those an entity feels may cause wide area impact.What if you do not agree with the third parties review of your

Organization	Yes or No	Question 2 Comment
		assessment? what evidence will be required to prove that you do not need to agree with their assessment?If an entity identifies a facility as critical does this require that the control center operating this facility must also have a full physical security plan per the requirements later in the standard?
Hydro One	Yes	Subsequent risk assessments should be performed every 36 months (to align with CIP requirements) instead of every 30 months. The FERC Order allows for the verification to be completed by NERC, the Regional Entity, an RC or another entity. The standard only identifies that the verification can be completed by a registered Planning Coordinator, Transmission Planner, or Reliabity Coordinator, or an entity with transmission planning and analysis experience; it does not mention NERC or the regional entity.
Portland General Electric	Yes	The following comments relate to suggested modifications for Requirements 1-3 -PGE believes the 90-day period to ensure verification of the risk assessment is too short. It will be difficult for every Transmission Owner to establish a contract with an unaffiliated verifying entity during the implementation time period. In addition, the current wording of the standard puts the obligation on the Transmission Owner to make sure that the assessment is done within 90 days, even though by definition they cannot have control over that timeline. Therefore, PGE proposes replacing the R2.2 language, "[t]he Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment," with the language, "[t]he Transmission Owner shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from the completion of the Requirement R1 risk assessment."In addition, Requirement R3 provides no mechanism for the Transmission Operator who operates a primary control center identified by a different Transmission Owner to disagree with that identification. PGE proposes including similar language to that in R2.3 to allow for the Transmission Operator to

Organization	Yes or No	Question 2 Comment
		document the technical basis for not identifying its primary control center as an asset to be protected.
Virginia State Corporation Commission	Yes	There does not seem to be any timeframe within which the initial assessment is to be completed under R1, nor when the 30 and 60 month periods for subsequent reassessments under R1.1 are to begin and conclude.
California ISO	Yes	We agree with the approach identified in R1 through R3, however we have the following comments regarding the SCOPE of the verification review required by R2.2: o The scope of the 3rd party verification is not well defined. What is the expectation and scope of the verification review? What level of quality is expected/required? Is the Transmission Owner responsible for scoping the verification process to ensure the review meets the required level of review? o Very little guidance is provided on the scope of the review. The scope of the review and verification work would need to be well understood before taking this verification work on. Is a technical analysis required as part of the review and verification process on the part of the 3rd party verifying the Transmission Owner's risk assessment and list of critical facilities, or is it simply to review the risk assessment and list of critical facilities that the Transmission Owner has provided to the 3rd party reviewer, based on their current knowledge of the transmission system from performing prior transmission planning studies? Will NERC be providing additional guidance regarding the scope of work required for verification by a 3rd party?
Western Area Power Administration	Yes	Western agrees with the approach of using Requirements R1 and R2 to identify whether an entity is subject to Requirements R4-R6. However, we suggest that the drafting team modify the term "risk assessment" to "BES impact assessment." In the physical security community, the term "risk assessment" generally refers to "The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel." See ASIS International, General Security Risk Assessment Guideline (2002), http://www.scnus.org/local_includes/downloads/9200.pdf. In its filing to FERC, NERC

Organization	Yes or No	Question 2 Comment
		can explain that it adopted the term “BES impact assessment” so it is clear that the initial evaluation is of risk to the BES if the substation is damaged or rendered inoperable.Western recommends revising R1 1.1 to: “Each Transmission Owner shall review their BES Impact Assessments once every 60 months for any transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection after completion of the initial assessment.” This would consolidate the two bulleted actions and make them equally applicable. We believe a 60 month interval would be a more appropriate period for this type of assessment.Western suggest the drafting team clarify requirement 2.1, which directs the Transmission Owner to select a Planning Coordinator, Transmission Planner, or Reliability Coordinator to conduct the third-party assessment; however, these NERC functional entity designations do not appear in the applicability section of the standard. We also suggest reconsidering the short 90-day period to ensure verification of the risk assessment. This may not allow every Transmission Owner to establish a contract with an unaffiliated verifying entity during the standard’s implementation time period.
Con Edison and Orange & Rockland	Yes	
Duke Energy	Yes	
Tampa Electric Company	Yes	
Tennessee Valley Authority	Yes	
American Electric Power	Yes	
American Transmission Company, LLC	Yes	

Organization	Yes or No	Question 2 Comment
City of Garland	Yes	
Clark Public Utilities	Yes	
Colorado Springs Utilities	Yes	
Edison Electric Institute	Yes	
Empire District Electric Company	Yes	
GridWise Alliance	Yes	
Manitoba Hydro	Yes	
Minnesota Power	Yes	
Minnkota Power Cooperative	Yes	
Modesto Irrigation District	Yes	
OPG	Yes	
Pepco Holdings Inc.	Yes	
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern	Yes	

Organization	Yes or No	Question 2 Comment
Company Generation and Energy Marketing		
The Empire District Electric Company	Yes	
The Empire District Electric Company	Yes	
California Public Utilities Commission: Safety and Enforcenment Division		In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive.The use of unaffiliated verifying experts is a positive element in the draft standard. In general, the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3, second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. With respect to Rule R1, Section 1.1, the drafting group should consider whether there should be language added to the standard detailing a process whereby the 30 or 60 month intervals should be accelerated in the event of serious intervening situations. With respect to Rule R2, Section 2.1, the description of “an entity that has transmission planning or analysis experience” is overly vague and should be further clarified, or that the use of this type of expert should be limited to certain small transmission owners. With respect to Rule R2, section 2.4, the language requiring “non-disclosure” agreements is important and a positive element in the draft standard.

3. **Requirements R4 through R6: The final three requirements of CIP-014-1 require (1) the evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified and verified according to the earlier requirements, (2) the development and implementation of a security plan(s) designed in response to the evaluation, and (3) a third party review of the evaluation and security plan(s) (as directed in the order). Do you agree with this approach? If not, please articulate how an alternative approach addresses the directives specified in the order on physical security.**

Summary Consideration: The SDT thanks all commenters. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Language to describe the responsible entities for Requirements R4 through R6 was made consistent. Changes were made to clarify factors to be considered by the responsible entity in Parts 4.2 and 4.3. Requirement R5 was reworded to clearly indicate the SDT's intent for security plans to be developed within 120 days of completing Requirement R2 and executed according to the timeline specified in the security plan. Requirement R6, Part 6.1 was changed to clearly indicate that one or more of the criteria must be met. Corresponding changes were made to the measures in the standard. Several additions were made to the Guidelines and Technical Basis section. A summary of comments and the SDT's response is provided:

- **Requirement R4. Various changes were recommended to the parts in Requirement R4 that describe factors to be considered in evaluating threats and vulnerabilities. Some commenters recommended deleting Parts 4.1 to 4.3. Some suggested adding additional language for clarity or to limit factors that must be considered.** Parts 4.1 through 4.3 provide considerations to be used by an entity in determining what threats may be 'realistically contemplated', as directed in the FERC Order. As written, Requirement R4 provides owners with appropriate requirements to develop a tailored evaluation process that takes into account factors such as location, size, function, existing protections, and attractiveness as a target. A clarifying change was made to Part 4.2 to now read "Prior history of attack…"
- **Requirement R4. A commenter recommended modifying Part 4.1 to focus the threat assessments on only those elements within a Transmission station or Transmission substation that affect the reliability of the BES.** The proposed standard satisfies FERC directives to address risks from physical attack on facilities as described in footnote 6 of the Order. A threat assessment must be performed for the entire Transmission station or Transmission substation. As noted in the Guidelines and Technical Basis section for Requirement R5, "While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site."
- **Requirement R5. Commenters asked for clarification on the 120-day time requirement to develop and implement a physical security plan, and the timeline required by Part 5.3 for implementing physical security enhancements or modifications.** Requirement R5 was reworded to clearly indicate the SDT's intentions. Physical security plans required by R5 must be developed within 120 calendar days of the completion of Requirement R2. This plan must include a timeline for executing physical security

enhancements and modifications according to Part 5.3, which may extend to a period determined by the responsible entity. The Guideline and Technical Basis section was also updated to clearly state the SDT's intentions.

- **Requirement R5. Commenters proposed alternate language for Part 5.1, indicated that requirements needed to be more specific, or proposed a specific technical solution.** The SDT accepted those revisions that it believes add clarity and are consistent with NERC Security Guidelines. The proposed standard meets the requirements of FERC's Order in a manner that supports reliability. FERC recognized that a "one-size-fits-all," prescriptive approach to protecting the Bulk Power System from physical security threats would not provide the most benefit. Like all standards, proposed CIP-014-1 is technology neutral. The SDT has provided several references and guiding documents in the guidelines section.
- **Requirement R5. Some commenters proposed removing Part 5.2 (Law enforcement contact and coordination information).** The SDT believes law enforcement contact and coordination information required by Part 5.2 is an essential element of a physical security plan and does not agree that it should be removed. EOP-004-2 includes law enforcement as an example of an organization to be included in an entity's event reporting Operating Plan, which may not meet the reliability objectives of a physical security plan developed to meet the requirements of CIP-014-1.
- **Requirement R5. A commenter recommended that the standard establish specific sequencing for the implementation of the physical security plans required in R5 to follow the review of the physical security plans required in R6.** The SDT believes the standard as written appropriately requires the responsible entities to implement physical security plans in a timely manner and does not support a establishing a timeline that places implementation after review. The SDT also recognizes that entities may develop the physical security plans and have them reviewed concurrently as explained in the Guidelines and Technical Basis section, which would satisfy the commenter's proposed sequencing. .
- **Requirement R6. Some commenters did not support the requirement for third party review or recommended changes to language or organizations listed in Part6.1.** The requirement for third party reviews satisfies the FERC directive and is intended to provide for an added level of physical security expertise beyond the responsible entity in the development of security plans. The SDT agreed with recommendations to change the list in Part 6.1 from numbers (6.1.X) to bullets to reflect their intent that an acceptable third party reviewer did not need to meet each criteria in the list. The SDT agrees that the credentials cited in Part 6.1 are not an exhaustive source of professional certifications. The SDT did not agree that the ERO should be the only authorized reviewer, and did not agree that any other specific additions to the list were necessary. The most appropriate third party reviewer for a given entity may vary based on the entity's specific circumstances and assets; collectively the list in Part 6.1 provides the necessary flexibility for all applicable entities. The suggested addition of a peer review group with physical security expertise is not explicitly necessary as such a reviewer could be utilized with ERO approval. A specific process is not required for the ERO to exercise its authority to approve a reviewing entity under Part 6.1.
- **Requirement R6. Commenters asked for clarification on whether third party reviews are required for plan revisions.** The SDT intends for all periodic review requirements for Requirements R4 and R5 to be addressed by meeting the 30 calendar month

review requirement of Requirement R1 and following the timelines in subsequent requirements. Changes or modifications made within the 30-month period are not specifically required to be reviewed by a third party.

- **Requirement R6. Some commenters indicated that a resolution process was needed or sought clarification for responding to reviewer recommendations.** The requirement for third party reviews as written provides for an added level of physical security expertise beyond the individual entity in the development of the required security plans. The Transmission Owner or Transmission Operator that created the physical security plan is ultimately responsible for physical security of the facility and thus makes the final determination on accepting the recommendations of a reviewer. The SDT believes that in documenting this determination as required in Part 6.3, the responsible entity should clearly explain their considerations and, if appropriate, an alternate approach that achieves the desired result.
- **Requirement R6. Commenters expressed concerns over potential for mishandling confidential or sensitive information.** The SDT agrees that the consequence of mishandling sensitive information is serious and has included methods that a responsible entity could use in complying with the standard in the Guidelines and Technical Basis section.
- **Requirement R6. A commenter proposed an exemption from Requirement R6 for federal entities that have an inspector general.** The SDT does not agree that the proposed exemption would meet the directives in FERC Order, Paragraph 11, which specifies that the review be conducted by an entity other than the owner or operator with appropriate physical security expertise. An Inspector General may be acceptable as a reviewer under Requirement R6 as long as they have the necessary expertise and is an unaffiliated third party. Please see clarifications in the Guidelines and Technical Basis section regarding affiliation.
- **Timelines for Requirements R5 and R6. Some commenters indicated that the standard did not allow sufficient time to complete the requirements.** The SDT believes that the timeline for Requirements R5 and R6 is aggressive but achievable.

Organization	Yes or No	Question 3 Comment
ACES Standards Collaborators	No	(1) We see a significant risk of the compromise of highly sensitive information created by Requirement R6 and question why the unaffiliated third party review cannot be integrated into the ERO compliance monitoring and enforcement processes. There is no compliance obligation on these third parties to complete the review within the required timelines, which could subject the TO to potential compliance violations. Furthermore, there is a limited set of companies with qualified personnel capable of performing this review. Given that all of the Transmission Owners will be working toward the same effective date of the standard, it is highly likely that a backlog of work would occur. Furthermore, review of the evaluations by consultants will increase the

Organization	Yes or No	Question 3 Comment
		the number of people with access to higly senstivie information. While this concern can be partially mitigated through confidentiality agreements, the more people that have the information, the higher the probability the information will be released, whether intentional or unintentional, to persons that should not have the information. To resolve this inssue, NERC and Regional Entities could hire qualified personnel to perform these reviews. NERC and Regional Entities could perform a spot check of the standard 90 days after the initial effective date. If NERC or the Regional Entity disagree with the approach or believe additional facilities should be added, RAI would give them the flexibility to treat the issue as not impactful to compliance as long as the TO resolve the issue within a certain time period. This approach would result in a reduced cost impact on industry and minimize the distribution of highly confidential information reducing the likelihood of information leaks. (2) How can the 'cost to benefit to risk to the BES' be measured consistently across each facility, region and risk? Does a Registered Entity have to authority to not implement a 'recommendation' from a third party based upon a cost to benefit to risk analysis? (3) Given that third parties are required to evaluate critical facility information, further guidance is needed for the required controls to prevent unintended release of highly sensitive and confidential information. What is the risk to the Registered Entity if the information does get leaked? Is this a violation to the Registered Entity, even if the leaked information was not caused by the Registered Entity? We are concerned that if this information were to be leaked, the Registered Entity could be liable for increased risk of attack, additional time and costs to address the leak and could impact the BES due to changes in operations from shutting down those facilities.(4) Part 4.2 has a potential "prove the negative" issue. How do you prove that you considered similar facilities particularly when similar facilities could includes other company's facilities. To resolve this issue we suggest replacing "similar" with "nearby facilities" or "asset owner's other facilities in the area". (5) Part 4.3 could be interpreted as requiring consideration of all threat and intelligence information including information that is not relevant to a given area. To remedy this issue, we recommend using the term "current and local" to describe the types of intelligence and threats that must be considered.(6) We believe that Part 5.2 is redundant to the EOP-004-2 - Event Reporting, especially Attachment 2 Event

Organization	Yes or No	Question 3 Comment
		Reporting Form line 4. Please consider removing and comparing the standard in its entirety to EOP-004-2 to avoid unnecessary duplication.(7) For Part 5.4, please modify the language to clarify that it only applies to facilities identified as a result of application of Requirements R1 and R2.(8) For Part 6.1 please modify "... from the following" to "... from one of the following". This will make it perfectly clear that only one entity must be selected.
Manitoba Hydro	No	(1) Manitoba Hydro has concerns about the need to have a third party to review or verify risk assessments and physical security plans. It is unclear at this point what measures or counter measures are being alluded to here as far as protecting critical assets such as lines and towers. This may potentially be financially burdensome as well as questionably effective.(2) Also missing in the standard is conflict resolution between a TO and this third party reviewer. Clarification should be provided on who weighs in on this and how NERC audits a system that has been verified by a third party. As currently drafted it appears that the third party reviewer/verifier would have no liability under the standard.
Texas RE	No	1. The sequence and timelines for R5 and R6 need to be reviewed. R5 states the TO "shall develop and implement" the security plan within 120 calendar days of completion of R2. R6 states the 3rd party evaluation can occur concurrently with or after completion of R5. It seems like the 3rd party evaluation should be completed before the plan is implemented in R5, otherwise the entity may be planning for or implementing measures that may not be appropriate for the risk level.2. R6 also 3. Also, who evaluates the implementation phase of security plan and whether or not it was implemented correctly or if the plan was effective? There should be an entity assigned for this task. There should be an exercise (like GridEx) to test the plan.4. The third party reviewer could be the same entity in R2 and R6. This could be a question of independence. It also does not indicate the third party actually verifies the implementation of the security plan(s) in R6. This does not permit the Compliance Enforcement Agency to place reliance upon the work of the third party.

Organization	Yes or No	Question 3 Comment
Georgia System Operations Corporation	No	o GSOC supports the comments submitted by both GTC and NRECA. o In addition, GSOC suggests in R4.2 changing "Prior history or attacks on" to Prior history of physical security related events at" to better describe the subrequirement. o GSOC suggests in R6, last sentence, changing the word "development" to "developed" in order to be consistent with the word "performed" in the same sentence.
Florida Keys Electric Cooperative	No	o It's unclear how an auditor will judge compliance with R4 and its subrequirementsas it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements. o R5.1 - FKEC strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement and resiliency will be next to impossible to audit. o 5.3 - After the word "modifications " add ",if any," as this is a possibile outcome. o R6 - Same as comments on R2 in Question 2 above. and R2.1. o R6.1.1 - NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides for the necessary skills under this standard. o R6.1.2 - It is highly unlikely that the ERO is not going to approve consultants for industry use. This should be removed. o R6.1.3 - All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed. o R6.1.4 - It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Flathead Electric Cooperative, Inc.	No	Again, do not support the third party review requirements. Already an auditable standard approach.
Florida Municipal Power Agency	No	Again, FMPA commends the SDT for a job well done. Just a few minor comments.See response to question 1 concerning use of the terms "control center" and "unaffiliated".CHANGE MANAGEMENT OF THE VULNERABILITY ASSESSMENT AND SECURITY PLANSimilar to our comments regarding change management of the risk

Organization	Yes or No	Question 3 Comment
		assessment, it is ambiguous as to how we would implement change management related to the vulnerability assessment and security plans.R4 has no periodicity requirement, but, instead seems to require responsible entities to continuously reevaluate their vulnerability assessments in response to events listed in bullets 4.1, 4.2 and 4.3. If the entity changes their vulnerability assessment to include new threats, does every revision require a new 3rd party review? How do we come to agreement what constitutes a valid "trigger" for a new vulnerability assessment? It seems to imply that each of us would need to have an independent 3rd party on retainer to review our assessment of every intelligence or threat warning from governmental or regulatory agencies, or new attacks that each entity becomes aware of. Is that the intent? If so, what consititues a "warning", e.g., is it an "official" warning through some sort of official channel, such as a NERC Alert? If so, what happens if an entity decided to act on an "unofficial warning", such as a media release, to revise their vulnerability assessment - would that also need a 3rd party review? FMPA suggest clarifying 4.3 with "Official intelligence or threat warnings ...".R5 seems overly ambitious. 120 days, or 4 months, is not a lot of time to perform a vulnerability assessment and develop and implement a security plan, especially in response to a newly identified threat vector/warning, and especially considering that a revised security plan may include capital investments in measures like new enclosures, vehice barriers, or the like. Is the intent that a security plan could be a phased approach, e.g., implement an interim security plan within 120 days while future improvements to that plan take longer? If so, then the language of the requirement ought to reflect that intent. FMPA suggest a modification to R5 such as: "... shall develop and implement the first phase of a documented physical security plan(s) ... within 120 calendar days ..."In addition, R5 does not seem to fit temporally with R2 and R4 well. R2 requires periodic risk assessments every 30/60 months. R4 seems to require changes to vulnerability assessments in response to newly known threat vectors. The timing of R5 refers to R2: "... within 120 calendar days following the completionof R2" with no reference to a revision to the vulnerability assessment. This causes FMPA to belevie that revisions to the security plan as a result of a new threat vector and a revised vulnerability assessment of R4 would not need to be required until 120 days following the next

Organization	Yes or No	Question 3 Comment
		periodic risk assessment of R2. Is that the intent?If that is the intent, if an entity chooses to revise the security plan earlier, would that then need an 3rd party verification at that time, or at the time of the periodic risk assessment?
Black Hills Corporation Entities	No	BHC has the same concern with R4 as expressed in the opening comment of the previous section regarding the definition risk assessment. The tailored evaluation required by FERC directive paragraph 8 introduces a probability of less than 100%, which is in conflict with prior NERC guidance on risk definition. As previously noted, if the unique probability of a threat is to be taken into consideration along with the impact, this change from CIP-002-3 expectation should be clearly highlighted. In addition, the inclusion of probability in the risk assessment will increase disagreements between unaffiliated entities, which will require a mechanism for resolution.BHC questions R4.2: The current language states “Prior history or attack”. BHC believes this opening should state “Prior history of attack” because the current language does not provide an indication of what ‘prior history’ is being referred to.BHC agrees with the AZPS suggestion that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions, which would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. BHC believes that the 120 day requirement for R5 should be limited to the development of the security plan, and that full implementation should be dependent on the complexity of the plan. Implementation timing of the entity’s plan should be approved by the applicable RC. Provisions could be added for temporarily derating the facility, if the implementation timing were considered by the RC to be excessively long. By mandating a 120 day implementation, entity’s security plans may be down-sized to meet the 120 day implementation window, rather than to meet the potential threats and vulnerabilities at the facility. If “implementing” only means the specific deliverables of R5.1, R5.2, R5.3, and R5.4 (i.e. the timeline required by R5.3 is created, but not executed), then “implementation” needs to be more clearly defined.BHC has a further concern that R5.1 language reads too close to the “Identify, Assess, Correct” language already remanded by FERC in the CIP v5 standards.

Organization	Yes or No	Question 3 Comment
		Alternative language for R5.1 might be "Resiliency or security measures designed to prevent potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." This simplification is not expected to change entities efforts, but could be more appealing to FERC.BHC agrees with the reasoning of AZPS to simplify R6.1 to read: "Each Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise." If this language consolidation is not acceptable, then alternatively recommend that Section 6.1.1 be expanded to include other similar certification providers, e.g. the National Sheriffs' Association Institute for Homeland Security offers a Certified homeland protection Professional (CHPP) designation (https://ndpci.us/certification/CHPP_Certifications.php), so as not to appear preferential.
City of Garland	No	Clarification - R6.2: Need to clarify that "completing the security plan(s)" does not include completing the tasks outlined in the time line developed in R5.3 - the time line is required to be complete as part of the plan but not the tasks in the time line.
Tennessee Valley Authority	No	Comment: Proposed language to be added to the end on Requirement 6:This Requirement shall not apply to any Federal corporation or agency that meets any of the criteria in Requirement 6.1 and that has an Inspector General, pursuant to the Inspector General Act Amendments of 1988, appointed by the President of the United States and charged with oversight responsibility for such Federal corporation or agency.Comment: Recommend adding "with electric utility experience" as a reviewer qualification to 6.1.3 and 6.1.4.Rationale: There should be a common standardizing qualification such as PSP, CPP, or electric utility experience that applies across the sub requirements of R6 that entities and the ERO can use as criteria to qualify unaffiliated third party reviewers.
Western Electricity Coordinating Council	No	From a compliance perspective, WECC notes that the criterion identified in R4 is too vague to enable a consistent approach across regions or even entities. Identifying a basic set of attack vectors that must be considered (ie: direct fire ballistic attack,

Organization	Yes or No	Question 3 Comment
		indirect fire attack, explosive device attack, vehicle-borne attack, arson/incendiary attack) fosters a far more consistent approach while allowing the entity the flexibility to tailor their assessment and security plan to the unique characteristics and threat landscape of their asset(s). WECC is concerned that the language of Requirement R5 is confusing or contratictory. Requirement R5 requires the applicable entity to "develop and implement" a documented physical security plan...within 120 calendar days following the completion of Requirement R2. However, part 5.3 requires a timeline for "implementing" the physical security enhancements and modifications specified in the physical security plan. WECC questions whether Requirement R5 requires the physical security plan to be "developed" or "developed and implemented" within 120 calendar days following the completion of Requirement R2. If Requirement R5 requires "development and implementation" within 120 calendar days following the completion of Requirement R2, what is the purpose of the timeline for implementing the physical security enhancements and modifications specified in the physical security plan required by part 5.3?
Georgia Transmission Corporation	No	-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.- GTC requests revision to the requirement language or addition of guidance around the phrasing of "unique charact
None	No	It is recognized that a one-size-fits all approach is not practical. However the proposed directives as to what should be included in physical security plans are so general that little is likely to change from current practices that are insufficient to protect very critical high risk substations. The only language directive in CIP-01401 is listed on Pg. 10, R5 para 5.1. More definitive guidelines must be outlined if improvements are to really be achieved.The utility industry has used real-time remote monitoring of substation equipment for reliability purposes for decades. Similar technology is available for the very important physical security function. The following sentence needs to be added at the end of paragraph 5.1. "Security measures must include isolation zones of sufficient size covering approaches to substations, in addition to monitoring inside substation fenced areas, to detect both attempted and actual

Organization	Yes or No	Question 3 Comment
		penetration of critical sites and the surrounding buffer areas. The areas must be patrolled with real time monitoring & assessment equipment designed to provide live and playback/recorded video that must be automatically presented to alarm station operators. Detection equipment must include gunshot detectors. Sufficient real-time surveillance must be provided to allow sufficient time to implement a tactical response plan to minimize and interrupt threats."
National Rural Electric Cooperative Association (NRECA)	No	It's unclear how an auditor will judge compliance with R4 and its subrequirements as it will be uncertain what an owner or operation is aware of regarding prior history, intelligence information, etc. The language should be revised to clarify the compliance expectations and also taking into consideration that each TO and TOP may have a varied exposure to the items identified in the requirements.R5.1 - NRECA strongly recommends the removal of "Resiliency or security" as this is not needed for the requirement, and resiliency will be next to impossible to audit.5.3 - After the word "modifications " add ",if any," as this is a possibile outcome.R6 - Same as comments on R2 in Question 2 above. and R2.1. R6.1.1 - NERC standards should not endorse, or appear to endorse, ASIS or its certifications in a requirement. This should be removed. There could be other certifications that an entity may have that provides for the necessary skills under this standard.R6.1.2 - It is highly unlikely that the ERO is going to approve consultants for industry use. This should be removed.R6.1.3 - All government agencies have physical security expertise for their own facilities; that doesn't mean they can be an adequate reviewer under this standard. This should be removed.R6.1.4 - It is unclear and not auditable whether an entity has demonstrated expertise. This language should be removed.
Los Angeles Department of Water and Power (LADWP)	No	LADWP requests the Drafting Team to make the following changes:- For R5, replace the word "implement" with "complete" to avoid confusion as to whether the plan needs to be implemented within the timeline provided- For R5.1, the word "Resiliency" needs to be defined in the standard to avoid any misinterpretation. Resiliency means different things to different people- For R5.1, add the language ", mitigate the impacts of," to the requirement as follows:"5.1. Resiliency or security measures designed to deter,

Organization	Yes or No	Question 3 Comment
		detect, delay, assess, communicate, mitigate the impacts of, and respond.....”- For R5.4, change the requirement language to read as follows:”5.4. Provisions to evaluate evolving physical threats to the Transmission station(s), Transmission substation(s), or primary control center(s), and their corresponding security counter measures. “This sub-requirement should allow for the TO to revise its already-reviewed security plan within the 30-month cycle without necessarily having to make arrangements for a third party review of the revised plan (although it may do so if TO so desires) and without creating an additional 30-month cycle review that the normal course - this is a matter of efficiency and due diligence to address evolving threats- For 6.1, as previously mentioned, the word “unaffiliated” needs to be defined in the standard to avoid any misinterpretation.- For 6.1.3, change the requirement as follows: “6.1.3. A governmental agency with physical security expertise, which could be a City Department in which the utility resides that requires a review to be performed.”This clarification allows for additional flexibility of independent governmental agencies reviews.- For 6.1.4, change the requirement as follows: “6.1.4. An entity or organization with demonstrated law enforcement, government, or military physical security expertise, such as the local police department in which the utility resides that requires a review to be performed.”This clarification allows for additional flexibility of independent entities or organizations reviews- For R6, add 6.1.5 with the following language: “6.1.5. A peer utility review group with demonstrated law enforcement, government, or military physical security expertise This clarification allows for additional flexibility of other Planning Coordinator, Transmission Planner or Reliability Coordinator review the work of their peers.In the alternative, expand to include Planning Coordinator, Transmission Planner or Reliability Coordinator with law enforcement, government, or military physical security expertise.- For 6.2, change the “90 calendar days” to “120 calendar days” to provide sufficient time to determine reasonable and sound recommendations.- For 6.3, chance the “90 calendar days” to “120 calendar days” to provide sufficient time to address any modifications recommended.

Organization	Yes or No	Question 3 Comment
New Brunswick Power Corporation	No	NB Power is concerned with the 120 day timeline to implement a physical security plan that would meet the third party verification requirements. Having limited knowledge of physical security issues NB Power will likely rely on the third party verifier to work with NB Power in developing a security plan. NB Power is not aware of any analysis that was done to ensure that there is enough capacity within the “physical security industry” to support the work load increase resulting from the approval of this standard and as such is concerned that 120 days may be insufficient.NB Power is concerned that it could be non-compliant with R6.2 if the third party fails to meet its obligation. While NB Power can mitigate the financial risk of that event it would still result in a recorded non-compliance.It is the opinion of NB Power that the proposed standard does not sufficiently address a disagreement resolution process between the TO and the unaffiliated reviewing 3rd party in requirement. NB Power believes that documenting the technical basis for not following the recommendations of the unaffiliated reviewing 3rd party without guidance on what constitutes valid technical reasons presents a compliance and enforcement gap where both the entity and an auditor may not be able to come to a consensus. NB Power suggests the SDT develop guidance concerning compliance and enforcement of this requirement indicating acceptable technical reasoning for not following the 3rd party’s recommendations.
Rayburn Country Electric Cooperative	No	Once the in scope facilities have been identified, it would be best for the entites to use the same resources for the evaluation of “Potential Threats” since this language has endless possibilities.i.e. Aerial attack, induced seismic events to name a few to illustrate "Potential". I favor the wording of "reasonable risks"The FBI, DOE or DHS should be involved in the discussion with the entities in lieu of a third party who is only subject to confidentiality agreements and also has interests beyond mitigating the true risks.
Ciy of Garland	No	R4 - Sub requirement 4.1 should be modified to include specific language focusing the security study to those elements within the substation that can affect the reliability of the BES. The security plan should protect those elements of the substation as

Organization	Yes or No	Question 3 Comment
		identified in the planning study in R1 that could cause the cascade or other unacceptable event identified in R1. Many substations identified in these studies are very large geographically and potentially very expensive to protect elements that may be located 30 to 50 feet above the ground. If these elements are determined to be critical they should be protected. If not, there is no justifiable reason to expend the resources to protect these devices. The security plans should concentrate on the protection of elements that could actually cause a cascading event, otherwise large expenditures may be made while adding no benefit or improvement to the reliability of the BES. R4.1 should read:4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) including the identified elements within the station, substation or control center, that need to be protected that could initiate the cascading collapse identified by the planning study in R1;Under both R4 and R5 clarification should be provided to the auditors affirming that auditors do not need the work papers, or backup information used in preparing the security plan, it is preferable auditors be allowed to only view the plan on site and not be allowed to take a copy of the plan for their files due to the sensitive nature of the security plan. Having copies of the security plans of critical targets consolidated into the files of the auditing entity increases the security risk to the plan and identified assets do to a security beach or accidental release of the file. While having one security plan of a critical location is a security risk in and of itself, having a compilation of security plans by one entity becomes a national security risk.R5 - states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." The "and implement" should be deleted. It should be made clear the facilities, additional employees or other measure identified in the plan are not required to be in place at the end of the 120 days. The requirement should be clearly stated that a timeline needs to be developed as part of the plan and the TO and TOP will implement the plan per the timeline identified in the plan. The implementation may require several years to get through budget cycles, procurement, installation and implementation.R6 - The standard should make clear the auditor is not

Organization	Yes or No	Question 3 Comment
		to audit the security plan for its content or appropriateness, but to confirm a security plan has been developed and that particular security plan has been reviewed by a qualified entity. It should also be clear that a TO could expand its actual security beyond that identified in the approved/reviewed plan without requiring an additional review of such modification. Example:The original, approved plan had card readers on the doors and cameras within the yard. During the 30 months until the next required review, the TO added motion detectors as additional security measures at the substation even though they were not required in the initial security plan. The installation of additional monitoring or security measures beyond those in the approved plan should not initiate the need for a new security plan or third party review.
Bonneville Power Administration	No	R4. BPA agrees with the requirements to develop a threat assessment and physical security plan. BPA also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers as noted in R6 (Section R6.1.3.) However, BPA requests that the drafting team clarify the scope and purpose of third party reviews should they remain as part of the standard. BPA disagrees that third party reviews will increase reliability and notes the draft standard exceeds the scope of the FERC order Paragraph 11. BPA believes that each entity is in the best position to evaluate threats to its facilities and determine appropriate mitigation plans. Nonetheless if third review is deemed necessary, BPA believes that it should be allowed to have another federal agency perform its third party review. In other words, for purposes of this standard, another federal agency would be deemed to be “unaffiliated” with BPA. Keeping this information within the federal government will decrease the risk of inappropriate disclosure of such information. BPA believes that non-disclosure agreements with non-federal parties may be a poor substitute for this because they can only be enforced once a disclosure is made. At that point, it is often too late and the information is available to a wider audience than intended. "R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each

Organization	Yes or No	Question 3 Comment
		Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: [VRF: High; Time-Horizon: Long-term Planning]" BPA recommends revising the 120 day requirement in R5 to 12 calendar months. Justification: This information is important to get right as security designs and enhancements will be built from this plan. 120 days is not be enough time to develop a complete and effective security plan and incorporate finalized threat assessments."R6 Each Transmission Owner that owns or operates a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. [VRF: Medium; Time-Horizon: Long-term Planning]" BPA recommends revising R6 first sentence to: "R6 Each Transmission Owner shall verify the risk assessment performed under requirement R4 by a third party entity other than the owner or operator." Justification: BPA believes the proposed revision fully aligns with the requirements of the FERC order by using the requirements of the FERC order. The introduction of a requirement of an unaffiliated reviewer is reaching beyond the requirements established by the FERC order, and this requirement will dilute the quality of a risk assessment. It will limit the types of entities that can perform an independent review, and directs use of resources that may not be capable of assessing all physical risks within an electrical facility. BPA proposes the word unaffiliated be removed from this standard and replaced with language that describes the degree of

Organization	Yes or No	Question 3 Comment
		separation from the facility owning entity to be considered a third party entity other than the owner or operator. Based on the definition provided in this draft "unaffiliated" is especially troublesome for federal government owned transmission networks and facilities because it could be interpreted as excluding the entire federal government from eligibility as a third party entity to the government transmission owner.Also, industry peer reviews should be encouraged and considered as meeting the requirement. Reviews by industry peers are known to be beneficial to the entity receiving the review and for the entity performing the review or audit. Enabling industry peer reviews would not only meet the intent of an independent review but also accelerate continuous learning and translation of the most effective security approaches into wide spread use. Please note that the FERC order only recommends this verification as it is stated as "should" and not as "shall."
Virginia State Corporation Commission	No	R4.2 requires each Transmission Owner of an identified facility to "consider" and "Prior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events." Is such consideration to be given to other "similar facilities" of the specific Transmission Owner or of any Transmission Owner anywhere in North America? How will such "consideration" be possible if the scope of such consideration is intended to be the latter? R5 is fine, but R6 suffers from the same ambiguity as R4.
Dominion	No	R5 and R6 are written for the initial risk assessment and don't necessarily apply for subsequent risk assessments. Is the expectation that 3rd party reviews be performed for R4 and R5 every time R1/R2 is run, particularly if there are no changes? Dominion recommends that the SDT modify this in the event the R1 list changes (ie: add stations) to require a subsequent R4/R5 reassessment. If stations drop off, or no change to R1 list for subsequent assessments, then subsequent R4/R5 reassessment is not required.R6 - Through continuous improvement processes and lessons learned, there will be expected changes to the security plan(s). What changes are allowed to the security plan(s) without triggering a 3rd party review?

Organization	Yes or No	Question 3 Comment
Bureau of Reclamation	No	Reclamation agrees with the requirements to develop a threat assessment and physical security plan. Reclamation also agrees with the inclusion of governmental agencies with physical security expertise as threat assessment and physical security plan reviewers. However, Reclamation does not believe that the proposed requirements will allow adequate time for a comprehensive review. Reclamation suggests that at least 180 days would be a more appropriate timeframe for a detailed threat analysis and physical security plan review. Reclamation also requests that the drafting team clarify the scope of third party reviews of these threat assesments and physical security plans, perhaps by adding additional detail to the Guidance and Technical Basis section. Reclamation is not convinced that third-party reviews will increase reliability. Reclamation believes that each entity is in the best position to evaultate threats to its facilities and determine appropriate mitigation plans. Reclamation is concerned that the well-intentioned third-party review mandated by the order could result in classified or national security related information falling into the wrong hands. Reclamation does not believe that non-disclosure agreements will adequately protect this sensitive information.Reclamation believes that audits by regional entities in essence provide a “third-party” review of an entity’s threat assessments and physical security plans.
SERC CIPC	No	Recommend adding electric utility experience to 6.1.3 and 6.1.4. Consider removing the requirement for CPP and PSP certifications. Rationale: Numerous other mandatory enforceable standards (e.g. MTSA, CFATS, and CT-PATS) that do not require specific certifications nor are we aware of similar certifications in cyber elsewhere in the CIP standards. Suggest clarification of “electric utility experience” and “physical security experience” to allow the ERO and registered entities to justifiably select authorized third party reviewers.
Northeast Power Coordinating Council	No	Regarding Part 5.1, the requirement states that the security measures should be designed to deter, detect, delay, assess, communicate and respond to potential physical threats. NPCC suggests removing the obligation to ‘deter’ from this Part and establish a separate Part that addresses deterrence and very basic specifics regarding

Organization	Yes or No	Question 3 Comment
		what constitutes deterrence. The new Part could describe how an entity should implement deterrence and consider some minimum auditable criteria; for example, Consider and Implement measures designed to deter potential physical threats including 1) perimeter control 2) motion detection 3) lighting 4) access control. In this manner the ambiguity surrounding the term 'deter' is eliminated. Part 5.3 should allow flexibility to modify the time line. Suggest that Entities should 1) have a master Physical Security Plan; 2) have the flexibility to accomplish mitigation activities associated with the results of the vulnerability assessment, and 3) capture those mitigation plans under a separate mitigation plan (similar to the action plans for Cyber Assets vulnerability assessments) or include "associated modifications to the time line".
Kansas City Power & Light	No	Same comments about "third-party" from Question 2.
NCPA Compliance Management Operating Committee	No	Same line of reasoning as given in the response to the question 2. If the Applicability Section were changed R1, R3, R4,and R5 could be combined together and R2 and R6 could be combined together. This simplifies the standard and gets to the heart of the Reliability Concern without creating a Consulting industry to perform third party reviews.(If you don't like the suggestion, maybe I found a new business opportunity)
Southern California Edison Company	No	SCE has concerns with Requirements R4, R5, and R6 that will be described below.With respect to Requirement R4, SCE notes that entities are required to "...conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)..." SCE requests the inclusion of additional guidance or examples of threats and potential vulnerabilities that an entity may want to consider. This will allow entities to perform a threat assessment and develop preventative measures that are commensurate with the intent of the standard. In addition, SCE requests additional guidance on physical security plans that allow for flexibility to deal with emergent threats. With respect to Requirement R5, SCE believes that in the guidance section, the drafting team should consider referencing standards that are used by security

Organization	Yes or No	Question 3 Comment
		professionals or organizations, in order to ensure that the criteria to identify appropriate countermeasures to potential threats and physical attacks are evaluated along similar themes across industry. SCE also requests that the team consider rephrasing R5.1 from “Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond...” to describe the control, to "...deter, detect and delay, and also assess, communicate, and respond..." With respect to Requirement R6, SCE requests that the team consider rewording Requirement R6.1 from “Each Transmission Owner and Transmission Operator...” to “Each Transmission Owner or Transmission Operator, with facilities identified as a result of R2,...”
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	No	Specifically, Vectren recommends that R6 be removed from the draft standard, for the reasons set out in this Comment. And that an approach similar to that used for evaluation of designations under CIP 002 Version 3 be adopted for review of the required risk assessment. Vectren urges FERC and NERC to establish clear criteria for verifiers, so that NERC auditors can apply a uniform set of criteria to their after the fact assessment of verifier qualifications. As written, these provisions lack the specificity necessary to provide clear direction to entities, increasing the risk of later non-compliance. Such a risk is ironic and unacceptable in requirements that purport to provide a review of risk assessments. Under these draft requirements entities have no assurance that any third party verifier they might select will be considered “qualified” by FERC, NERC or NERC auditors who might review the results later - leaving entities at grave risk of compliance violations if FERC, NERC or any other regulatory body later disagrees with the entity’s selection of a third party verifier. Vectren strongly urges NERC and FERC to establish criteria for those who might seek to be designated third party verifiers, rather than leave assessment of qualifications to an after the fact review during a NERC audit or spot check. A lack of certainty leads here by necessity to a lack of confidence in the result, which Vectren surmises was not the intent of FERC or the drafters.

Organization	Yes or No	Question 3 Comment
Southwest Power Pool Regional Entity	No	SPPRE disagrees with the inclusion of Requirement 4.2. Prior history is not a predictor of future events and could result in critical facilities not being protected until after a sucessful first damaging attack with adverse BES reliability impact. Requirement 5.3 should be a project plan with measurable milestones for implementing the physical security enhancements and modifications.
Salt River Project	No	SRP supports comments submitted by APPA with the following additions:Third Party Verifiers:SRP recommends removal of the concept of third party verifiers and adherence to the existing, and well-functioning, audit program of FERC, NERC and the Regional Entities. If, at any time, modification to the compliance and audit program in regards to any or all of the standards are deemed necessary, such modification can be proposed, evaluated and implemented with due process to ensure no unintended adverse impacts. SRP is concerned that use of third party verifiers to verify, or opine on compliance, both undermines the foundational structure of the FERC/NERC/Regional Entity audit program and introduces additional risk for the safeguarding of critical facility information on physical threats and vulnerabilities. The national audit program for the mandatory Reliability Standards is founded on compliance, self-reporting and a range of audit types, including spot checks and regularly-scheduled audits by NERC and Regional Entities. There are no facts to support abandonment of this foundation in favor of the introduction of a non-authoritative mid-layer of inspection by third parties. Third party verifiers are not authorized to verify compliance. As such, a Registered Entity derives no concrete benefit from a third party verifier's expressions of agreement or disagreement with the Registered Entity's compliance activities. Notwithstanding the theoretical value of another's opinions on whether one has properly or fully complied with the requirements of CIP-014, there are sound and compelling reasons to forego requiring such opinions at the expense of owners. On the other hand, as demonstrated with other standards, Registered Entities readily retain expert consultants as needed to help them evaluate and resolve all manner of compliance challenges. This standard is no different in the sense that outside subject matter experts already are being retained as needed by the party bearing compliance

Organization	Yes or No	Question 3 Comment
		responsibilities.Introducing third parties does not guarantee value-added subject matter experts versed in the nuanced and individualistic profiles on critical facilities. The Transmission Owner already is required both by law and sound business practices to be versed in physical security risks and potential vulnerabilities of critical facilities. The owner both knows which are its critical facilities and is best suited to identify the optimal means and methods to protect them. There are overwhelming incentives for Registered Entities to evaluate and take all appropriate steps to ensure continued reliability of the bulk electric system and reliable service to electric customers. Critically, neither the owner nor FERC/NERC/Regional Entities can rely on the findings of third party verifiers: the approved program of compliance audits will continue regardless and without regard to the findings of third party verifiers.Confidentially of the highly sensitive information produced, gathered, used and maintained for compliance with this standard is critical. Wholesale introduction of a new subset of entities who would routinely gain access to such information poses additional challenges to information safekeeping. Absent demonstrable need, granting access to physical risk and vulnerabilities information introduces unnecessary risk. With any access, vulnerabilities for inappropriate use or further unauthorized access occur. Prudent industry practices dictate non-disclosure absent demonstrable need to know or compelling benefits from such disclosure. Here there is no record of need or benefits.
David Kiguel	No	Sub-requirement 6.1.1: While Certified Protection Professional (CPP) or Physical Security Professional (PSP) might be recognized certifications in the U.S.A., that is not necessarily the case across the Canadian Provinces. Recommend to add: “or equivalent in those jurisdictions where such certifications are not recognized.”Sub-requirement 6.4: In addition to the non-disclosure agreements referred to in this sub-requirement, the standard should specify that the reviewing individuals having access to the confidential information must have security clearance and training, similar to the requirement in other CIP standards. Also, the security clearance must be obtained according to the established procedures in the respective jurisdiction.

Organization	Yes or No	Question 3 Comment
Encari	No	The approach taken by the Nuclear Regulatory Commission, which prescribes specific physical protections for nuclear plants and materials in 10 CFR Part 73, is instructive. Applicable Transmission Facilities, which are subject to common potential threats and vulnerabilities, warrant minimum physical security protective measures. Physical security plans should incorporate those prescribed protective measures unless a responsible entity can establish that its validated security plan provides a comparable level of protection required by the Standard.
Hydro QuÃ©bec TransÃ‰nergie	No	The same comments regarding the term "unaffiliated" in Question 2 above apply to R6.HQT believes that the SDT should remain general about the security measures that should be put in place. Requirement R5.1 states "Resiliency or security measures designed to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4." We believe that rather than the standard dictate what type of measures are to be implemented, it should be rephrased to remain general and use similar language that is used in paragraph 9 of the FERC order. Suggest rewording the requirement to "Resiliency or security measures designed to protect against potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.".
Foundation for Resilient Societies	No	The third party review is not adequately specified. The Joint U.S.-Canada Outage Tasf Force Report (April 2004) determined that lack of Reliability Coordinator oversight, and legal authority, contributed to inadequate supervision of transmission operators, and reduced visibility of regional inadequacies. See our comment to Question 1 for our view that Reliability Coordinators and Balancing Authorities must be involved.
FortisBC	No	The third party review of the security plan does not guarantee an objective evaluation as they would be funded by the requesting entity. The standard could state that the entity should follow an industry standard technical guideline.The audit provides an independent review of an entity's application of the industry standard technical

Organization	Yes or No	Question 3 Comment
		guideline and therefore, an additional third party review should not be required as described in R6.
Tri-State Generation and Transmission Association, Inc.	No	Tri-State disagrees that the FERC order specifically forces the drafting team to have a requirement for 3rd party verification. The order uses the word “should,” not “shall” or “require.” Tri-State would argue that 3rd party verification would/will occur during scheduled audit times. Again if the drafting team feels a need to require an additional 3rd party verification, it should require the Regional Entity or Reliability Coordinator to request the plans.
Consumers Energy Company	No	We agree to the approach, however, our concern is around protection of information shared between the entity and the third party. There should be a requirement within the standard that requires the third parties to protect the information and not leave it up to the entities.
Public Utitliy District No. 1 of Cowlitz County, WA	No	We are very concerned with the preferential endorsement this Standard affords to ASIS International. We know of at least one other security organization that offers a security certification: the Certified Homeland Protection Professional (CHPP) designation form the National Sheriffs' Association Institute for Homeland Security. If this requirement is left unchanged, FERC's statutory obligation in determining a proposed reliability standard is "not unduly discriminatory or preferential" may trigger the standard to be remanded back to NERC. It is for this concern, and only this concern Cowlitz votes negative. However, Cowlitz plans to vote affirmative in the final Ballot, regardless of any concerns to allow NERC to meet FERC requirements.
Cooper Compliance Corp	No	We do not support the Standard for the same reason above. We do not support a third party review requirement other than that of the existing Standards. That is a review by FERC, NERC or the appropriate region.

Organization	Yes or No	Question 3 Comment
self	No	While the reqirement for unafflilated third party verification of the security plan is required by the FERC order, I believe the mandate will lead to future security compromises.
Western Area Power Administration	Yes	: We recommend striking the qualifier regarding the ASIS “Certified Protection Professional or Physical Security Professional” from the standard R6-6.1.1 as it is inclusive of only one organization and may not provide the best support for each entity . Simply having these certifications does not guarantee the necessary knowledge to perform this unique work. We believe the language does not support the intent of the FERC Order as identified in paragraph 11.We request the Drafting Team clarify the scope of the third party review process identified in R6 and tie the requirement to a specific and established method as consistent in accepted practices, such as the ISO processes. We recommend the third party review process be clarified as a review of the primary entity’s adherence to their established processes in evaluating threats and vulnerably, as well as their security plan(s). We believe the current audits conducted by the regional entities satisfy the third party review process as identified in the FERC Order, paragraph 11.We do not believe R6-6.4 adequately protects the sensitive information contained in the risk, threat, and vulnerability assessments, or the security plan(s). These reports may contain sensitive and/or classified information, or otherwise information that if released would jeopardize the BES, with little to no penalty for an offending party.
Utility Services	Yes	1. R4, what is the time frame for the evaluations? Is this to be conducted during the 30 or 60 month cycle outlined in R2 or more frequently? 2. R6.1, These are all “or” statements and 6.1.1 through 6.1.4 should be bullets, not numbers (this is outlined in the CIP-002-5 page 6, and should maintain consistency with the CIP standards format). 3. R6, Does the ERO have to approve of the third party reviewer? Is there going to be a criteria to determine “demonstrated physical security expertise”?
ATCO Electric	Yes	AET agrees with the flexible approach outlined by the draft standard and respectfully offers these following comment for the drafting team’s consideration:R4 - Please

Organization	Yes or No	Question 3 Comment
		consider altering the wording of the final sentence of R4 to "The evaluation shall consider, at a minimum, the following:". This allows additional flexibility for entities with existing physical security assessment programs to continue to include those extra elements within their plans.R5 - For the timeframe dependency please consider altering the dependent requirement to R4 instead of R2. Within the rationale section the drafting team concedes that R4 must be completed prior to commencing R5 and the drafting team also states that R4 does not state when the evaluation must occur, only that it must occur in time to meet R5. AET respectfully suggests that a linear progression be established just as in R1, R2, and R3. This would require a timeline be added to R4 for the completion of the physical security risk assessment (AET suggests 120 calendar days from the completion of R2). AET also respectfully suggests that R5 then be made dependent on the completion of R4 (AET suggest 120 calendar days from the completion of R4).R6 - Please consider the removal of the required certifications in R6.1.1. The FERC order specifies that the risk assessment be reviewed by "[...] or another entity with appropriate expertise" and does not specify any particular qualifications. In addition, no other CIP standard calls for specific certifications or qualifications. Neither engineering focused requirements (e.g. CIP-002) or cyber security focused requirements (e.g. CIP-003, 005, 007) specify that those requirements be reviewed or implemented by designated engineers or certified security practitioners (e.g. CISSP). The due diligence required of the entity will determine the level of rigor that that entity is comfortable with defending and should not be included in the standard.
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.R4 CLARITY - Under R4, combining the applicability of this requirement to both TOs and TOPs with applicable control centers within a single sentence is confusing and could be read to imply that a TOP that is affiliated with a TO must arrange for a separate third party review. We recommend

Organization	Yes or No	Question 3 Comment
		revising R4 to read as follows:R4 Each Transmission Owner that owns a Transmission station or Transmission substation identified in Requirement R1 and verified according to Requirement R2, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s) and Transmission substation(s), identified in Requirement R1 and verified according to Requirement R2. Each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to their primary control center identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning] R4.2 TYPO - Please change: "Prior history or attack..." to "Prior history OF attack..." Make conforming edits to the RSAW. 30-MONTH CYCLE - Identification of new threats and vulnerabilities in R5.4 does not change the 30-month cycle for conducting reliability studies and security evaluations: The standard needs to make clear that the security plan needs to take into account threats and vulnerabilities that are known at the time the plan is developed and the approved plan is capable of addressing new threats and vulnerabilities as they emerge, but that there is no NERC requirement to revise the plan between 30 month cycles and for the NERC CEA to audit such revisions. The TO should apply its existing security plans and procedures to evaluate and mitigate evolving security threats. The TO may also revise the security plan in mid-cycle if it so chooses without arranging for a third party review, but that action does not obviate its obligation to conduct the "subsequent" risk assessment and threat evaluation and security plan on the 30 month cycle. The CEA will audit the processes the TO uses to develop its plans, rather than the content of the plans.REQUIREMENT R5 CLARITY - R5 states in part that each TO and TOP "shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2." Please change "implement" to "complete." The use of implement can easily be read to require the actual

Organization	Yes or No	Question 3 Comment
		implementation of physical security measures within 120 days, rather than the completion of the security plan, starting the 90 day clock for unaffiliated third party review under R6. In contrast, R6 states that: "The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5."
Arizona Public Service Company	Yes	AZPS generally agrees with the approach of the standard as drafted. The following comments relate to suggested modifications or clarifications for Requirements 4-6.AZPS is concerned that Requirement 4.3, which requires the Transmission Owner to evaluate threat warnings from a myriad of sources, will result in inconsistent application by entities. The threat sources need to be consistent, and the threats evaluated must be relevant. AZPS suggests that a sector specific threat source be utilized to aggregate and disseminate threat information to ensure that relevant and timely data is analyzed consistently across the regions. This would also improve the auditability of the standard as well by removing the subjectivity associated with an unbounded number of threat sources. Requirement 6 requires Transmission Owners to secure a third-party review of the security plan developed under Requirements 4 and 5. AZPS strongly supports the development of security measures to protect critical substations. However, AZPS believes that requirements 6.1.1 through 6.1.4 add a level of specificity that does not provide an improved reliability benefit and has the potential to create a bottleneck that would make compliance within the short 90-day timeframe very difficult. AZPS contends that the most important quality of the third party reviewer is electric industry physical security expertise. Further, AZPS does not believe that the CPP or PSP certifications provide additional value from a realiability standpoint since neither certification has a sector specific focus. For these reasons AZPS would suggest that 6.1 be simplified to read: "Each Transmission Owner and Transmission Operator shall select an unaffiliated third-party reviewer with electric industry physical security expertise."
Tampa Electric Company	Yes	Comments to R5Tampa Electric Company appreciates the excellent work of the standard drafting team (SDT). They and their support staffs have evidently worked

Organization	Yes or No	Question 3 Comment
		very hard to produce in a very short time a family of documents that create a workable framework for improving the physical security of Transmission substations and primary Control Centers. We also commend NERC and the SDT for reaching out to the industry through a live a technical conference and by conducting a series Webinars in local and national venues. Moreover, we fully support the intent of the SDT as it has been articulated so well in the technical conference, in NERC and FRCC Webinars and in EEI and NATF conference calls. Unfortunately, there is a critical ambiguity in the text of requirement R5 that is problematic and needs to be addressed by the SDT. Our main concern is that requirement R5 literally reads that all provisions of the security plans for our primary control center and for all our substations and switchyards, including the installation and construction of any physical security upgrades, must be completed "within 120 calendar days following the completion of Requirement R2." Such a requirement may well be impossible to meet depending on the extent of the upgrades, the need for facility outages, and the number of locations that are affected.Members of the SDT have made it very clear in the Webinars and conference calls that they did not intend this result. Instead, the SDT intended to require registered entities, "within 120 calendar days following the completion of Requirement R2," to develop and document plans that include definite timelines for completing any security upgrades that are necessary to protect against the vulnerabilities and threats that are identified under requirement R4. Given that the text of R5 is contrary to the intent of the SDT, Tampa Electric urges the SDT to clarify that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work. This clarification can be accomplished in the guidance document to the standard or by our preference, editing the text of the standard and issue a revised standard for a second ballot. Removing "and implement" from the text of requirement R5 should remove the ambiguity and conform the text to the intent of the SDT. This edit, combined with R5.3 expresses the SDT's intent on this issue: R5. Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to

Organization	Yes or No	Question 3 Comment
		Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days following the completion of Requirement R2. The physical security plan(s) shall include the following attributes: [VRF: High; Timeâ€ Horizon: Longâ€ term Planning]5.3. A timeline for implementing the physical security enhancements and modifications specified in the physical security plan.
FirstEnergy	Yes	FirstEnergy supports the proposed requirements R4 through R6 but offers two comments: 1) In regard to the inclusion of "primary control centers," we suggest the team add language within the Guidelines and Technical Basis section for requirement R4 and potentially the inclusion of an additional FAQ item to document some of the team's feedback provided during the webinar sessions. During the webinar the team provided a good explanation of how CIP-014 is uniquely different than physical protections provided under CIP-006 and that CIP-014 provides perimeter protection of the primary control center location or site and not just the subset of the control center that may house cyber assets protected under CIP-006. 2) Regarding requirement R5, during the industry webinars it became evident that there is some confusion associated with the word "implement" as used in the statement "shall develop and implement a documented security plan(s)" and that some industry stakeholders questioned if implement intended completion of all identified tasks stated within the plan(s). While FirstEnergy understood the requirement as described by the team during the webinars, to alleviate any confusion and better clarify the intended application, FirstEnergy suggests changing "implement" to "initiate" or "issue" so that it reads "shall develop and initiate a documented security plan(s)". This wording may better align with part 5.3 and the guidance provided in the Guidelines and Technical Basis section that states "Entities have the flexibility to prioritize the implementation of the various resiliency or security measures in their security plan according to risk, resources, or other factors."

Organization	Yes or No	Question 3 Comment
Idaho Power Co.	Yes	Further clarification is needed on several points. 4.2 & 4.3 leave open much room for interpretation under audit to say you did or didn't consider a particular source or threat. There is also some consternation over the use of "potential threat" in this requirement. There are a great many potential threats many that are so remote and nearly impossible to protect against that the risk does not outweigh the cost. It seems like these sub-requirements are a potential audit findings trap by the way they are worded. There are also no criteria specified for what the unaffiliated third party will be looking for in their review of the entity's evaluation. There is a great deal of concern for how these third parties will be able to handle or be willing to handle the influx of these reviews especially considering the short 90 day timeframe listed in 6.2.
Public Utility District No. 2 of Grant County, WA	Yes	GCPD appreciates the flexibility built into the Standard language that allows tailored evaluations of potential threats and vulnerabilities to its own facilities. GCPD supports APPA's suggested edits to the Standard to enhance clarity of requirements under R4, R4.1 & R4.2.In addition, APPA's suggested removal of “and implement” under R5 clarifies that the intent of R5 is to develop the physical security plan, not fully implement the plan within 120 calendar days. This would better align the Standard language contained in R5.3.
Vermont Transco LLC	Yes	how long will and entity have to complete their plans designed due to the evaluation of threats? It appears that the standard is saying that you must develop a plan and a timeline to complete your actions associated with the plan. What if a timeline needs to be adjusted at some point, will an entity have to notify their RRO? Or just track all changes and their need to provide to an auditor during a full audit of the standard?
Portland General Electric	Yes	In Requirement R4 the phrase “owns or operates” is used for the first time. If Transmission Owner Entity A is also a Transmission Operator of a line it does not own, and that line was identified by Transmission Owner Entity B in Requirement R1 and verified according to Requirement R2, Entity A could be responsible for evaluating and protecting that line under this wording. However, there is no mechanism built into the standard to communicate this information or to allow the Transmission Operator to

Organization	Yes or No	Question 3 Comment
		dispute the decision. In addition, Requirement R4.2 should be changed to "[p]rior history of attack."In addition, in Requirement R4.3, the current wording places an unrealistic and unclear burden on every Transmission Owner to monitor intelligence or threat warnings from an open-ended list of sources. We recommend changing the wording from "[i]intelligence or threat warnings from sources" to "[i]intelligence or threat warnings received from sources" to narrow the obligation to information that the Transmission Owner actually received from its monitoring activities.In addition, in Requirement R5, the phrase "owns or has operational control over" is used for the first time. It's not clear why this needs to be different from the "owns or operates" in Requirement R4. Consistent terms should be used to decrease potential confusion.In addition, as above, PGE believes that the 90-day period to review each entity's evaluation and security plan is too short. Again, we propose replacing the R6.2 language, "[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5," with the language, "[t]he Transmission Owner or Transmission Operator, respectively, shall ensure that any agreement executed with the unaffiliated verifying entity stipulate that the verification be completed by a date that is not later than 90 calendar days from completing the security plan(s) developed in Requirement R5."
MidAmerican Energy Holding Company	Yes	MEHC agrees with the R4 through R6 approach. However, MEHC suggests the following changes to improve the standards as written: The following rewording of R5 is recommended to clarify that the "build out" of security enhancement schedule. R5 Each Transmission Owner that owns or has operational control of a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The plan shall be completed

Organization	Yes or No	Question 3 Comment
		within 120 calendar days following the completion of Requirement R2. Implementation of the plan shall be as documented in the plan.
NRG Energy, Inc.	Yes	NRG agrees the approach described in Requirements 4 through 6 addresses the directives specified in FERC Docket No. RD14-6-000. However, NRG does have concerns with the standard as currently composed and offers the following points it believes will improve the standard if implemented: o R5.1 provides no guidelines or examples of how to combat certain threats, or even what threat thresholds require accounting for. NRG appreciates the flexibility built into the requirement. However, NRG is concerned this flexibility could result in "interpretation" issues during future audits of compliance with the standard. o The ability to meet the time horizon commitment for providing the third party assessment of the vulnerabilities and security plan are contingent upon the availability of certified parties that can adequately perform these assessments. NRG is concerned there may be a lack of qualified resources available to the industry to complete the necessary reviews within the required time frame. o Because the reliability of the bulk power system depends on numerous susbstations all across the nation, it would be more effective to increase the monitoring of the grid to ensure timely, effective re-routing of power when a disruption occurs. o Minimum physical standards should be established within the security plan that include industrial standard chain link fencing with barbed wire topguards; gates secured with chains and locks (not the alloy metal collar around a post); signage that clearly states No Trespassing every 100 ft., or on each perimeter side at small footprints; cameras that are monitored by the appropriate transmission control center, security control center or a contract central monitoring service and capable night viewing to be able to identify intruders.
Minnesota Power	Yes	Overall Minnesota Power agrees with the approach laid out by the Standard Drafting Team in Requirements 4-6, but requests that the SDT consider modifying the wording of R5.1 as follows.Resiliency or security measures designed to deter, detect, delay, assess, communicate, or respond to potential physical threats and vulnerabilities based on the results of the evaluation conducted in Requirement R4.An auditor could

Organization	Yes or No	Question 3 Comment
		interpret the use of “and” in “...deter, detect, delay, assess, communicate, and respond...” to mean that each resiliency or security measure be designed to meet all of these, where we believe and hope that the intent of the sub-Requirement is that the resiliency or security measure identified in the physical security plan be designed to “...deter, detect, delay, assess, communicate, or respond...”, while recognizing that it may meet more than one.
Xcel Energy	Yes	Overall Xcel Energy agrees with the approach, but we offer the following items for consideration of the Standard Drafting Team.The rational for R4 and R5.1 indicate that there is no required timeframe to complete the evaluation of the potential threats and vulnerabilities to identified facilities, but it does indicate the linkage of completing this when the physical security plan developed as part of R5 and within 120 days of completion of R2. We suggest that it might be more efficient to combine R4 and R5 or clearly show the linkage to reduce confusion about the timing of these two activities. Maybe the standard should require entities to develop a physical security plan after the risk assessment is completed, not after a verification of facilities as specified in R2. If R2 returns a null set, this seems ambiguous as we may still be required to have a physical security plan, even if blank. Since R4 would only be considered applicable if the R2 risk assessment process identifies facilities, referencing R4 in R5 would seem more intuitive.R5.2 states that the physical security plan must include law enforcement’s contact and coordination information. However, guidance on law enforcement and coordination has already been established with the adoption of EOP-004-2. It is also unclear by what is meant by “coordination”. Since reporting a physical threat to a Facility is a requirement of EOP-004-2 and in order to remove ambiguity around the word coordination, we propose changing R5.2 to read “notification of law enforcement consistent with EOP-004-2”. This would avoid potential confusion whether the R5.2 requirement is different than the EOP-004-2 requirement.R6.1, While there will be some regional variances, if an entity spans multiple regions or even some governmental agency jurisdictions, what protection does an entity have against reviewer discrepancies or differences? For example, the Xcel Energy registered entities anticipate using a common risk assessment methodology, and similar security plans. It

Organization	Yes or No	Question 3 Comment
		would be efficient to have a single evaluator provide the review for all three Xcel Energy registered entities. It would also be important for Regional Entities to apply consistent criteria when auditing the risk assessments and security plans.R6.1.2, if the ERO does not meet any or some parts of the criteria established in R6.1, it is uncertain how the ERO will be able to determine and approve an organization that does. Our security department, like the departments at other utilities of similar size, consists of a mix of multiple CPP and/or PSP holders, prior law enforcement professionals and several career military experts, including nuclear military asset security. It would seem that resources within the industry are the most knowledgeable resources available to evaluate physical security plans, given the criteria, and would have more utility specific knowledge than outside entities. Similar to our comments regarding R2.1, since the industry has the most knowledge on threats and vulnerabilities, and means to prevent them, we again propose adding an option to allow for industry (but non-affiliated) peer review of the physical security evaluation, either directly or through a group organization such as the North American Transmission Forum. Allowing peer review is likely to assist in identifying and disseminating best practices, thereby improving security. R6.3. Similar to our comments regarding R2.3, if no recommendations are made for changes to the evaluation by the unaffiliated reviewing entity, does this conclusion need be documented? Since some of VRFs are built off this requirement, it would seem to follow that all aspects be included to ensure certainty for the industry.
Pacific Gas and Electric Company	Yes	R4 (pg. 9) "...shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s)..." Comment: Consider stating "...conduct a physical security risk assessment to identify and evaluate potential threats and vulnerabilities..." The assessment should identify the potential threats and vulnerabilities to evaluate and implement the necessary protective, detective and corrective countermeasures R5 (pg. 10) states to develop and implement a documented security plan (s) within 120 calendar days of completion of R2 (unaffiliated third party verify the risk assessment form R1). Furthermore, R5.1 states to address the potential threats and vulnerabilities from R4. 120 days to implement

Organization	Yes or No	Question 3 Comment
		the countermeasures may not be enough time (logistics, procurement, installation timelines, approvals, etc.). Comment: Could they say "...shall develop and begin implementation of a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) within 120 calendar days..." because in R5.3 it requires a timeline for implementing the enhancements. 6.1.1. (pg.11) "An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification." Comment: Shouldn't require a specific certification, should say something like "The third party must include in their review the qualifications of the staff performing the review." R6.1.2 (pg. 11) "An entity or organization approved by the ERO." Comment: What criteria is the ERO using to approve entities or organizations? The approval process needs to be spelled out. R6.1.3 (pg. 11) "An entity or organization with demonstrated law enforcement, government, or military physical security expertise" Comment: Does this mean we can use Law Enforcement agencies or firms with retired law enforcement personnel?
ReliabilityFirst	Yes	ReliabilityFirst supplies the following comments for consideration:1. Requirement R5 - ReliabilityFirst requests clarification on why the term "primary control center" is used throughout the document instead of just "control center", as it seems both a primary and secondary control center would be of equal importance (and have similar vulnerabilities) to reliability.
PPL NERC Registered Affiliates	Yes	Requirement 5:In the VSL table, does implemented mean complete execution of the plan including any necessary construction, or does it mean having initiated the plan but not necessarily completed all planned construction? There are only 10 days between VSLs. Requirement 6:1. Similar to Requirement 2.3, the sub-requirements under Requirement 6.1 should be bullets, not individual sub-requirements. 2. Does R6 require subsequent third-party reviews when the security plan is revised? If so, what are the criteria?

Organization	Yes or No	Question 3 Comment
San Diego Gas & Electric	Yes	SDG&E agrees that an evaluation of potential threats and vulnerabilities of a physical attack to the facilities identified in R1 through R3 of the Standard is appropriate. Security threats and vulnerabilities can, and will vary from location to location and such differences must be accounted for in a robust security plan. It is appropriate and necessary that the Standard not mandate a one-size-fits-all approach, but requires entities to take into account the unique characteristics of each facility. SDG&E understands the Federal Energy Regulatory Commission's concern addressed by its Paragraph 11 directive that the Standard must have the analysis verified by an independent third party. While SDG&E believes it has in-house experts capable of performing such an analysis (as required by R4) and developing a Physical Security plan (as required by R5) adequately, SDG&E appreciates that verification by a third party, essentially a "second opinion," can serve to ensure a robust analysis of the physical security threats and vulnerabilities of facilities identified in Requirements R1 through R3. SDG&E appreciates the broad definition under R6.1 of what qualifies as a "unaffiliated third party reviewer." A list that unnecessarily limits possible reviewers could: 1) result in a bottleneck as too few potential reviewers are available for the industry to use; and 2) result in increased costs and a tight market for reviewers results in higher prices for their services.
Seattle City Light	Yes	Seattle City Light supports the Question 3 comments of APPA.
Seminole Electric Cooperative, Inc.	Yes	Seminole supports the comments by NRECA. Additionally, Seminole agrees with this approach. Requirements R4.1, 4.2, and 4.3 should be moved to the guidelines and technical basis as there is excessive flexibility provided to the auditor for concluding whether the evaluation is adequate and potential that an auditor may choose to determine that identification of events was inadequate. R5.2 requiring law enforcement contact information is redundant with EOP-004-2 R1. If an entity has a qualified third party perform the R5 security planning on behalf of or in cooperation with the registered entity, does this also meet the requirement R5? R6.4 is redundant with the information protection requirements in CIP-011-1. It would be appropriate to

Organization	Yes or No	Question 3 Comment
		note that this information is included in the materials subject to enforcement under CIP-011-1 R
Northeast Utilities	Yes	Suggest standard allow entities to have a Master Physical Security Plan and that the standard provide for flexibility to accomplish mitigation activities associated with the results of vulnerability assessments and capture those under a separate mitigation plan (similar to the action plans associated to vulnerability assessments being conducted on Cyber Assets).
PNM Resources	Yes	Support the comments submitted by EEI
Hydro One	Yes	The Standard allows the TO and TOP sufficient flexibility to complete R4, R5 and R6.
Con Edison and Orange & Rockland	Yes	
Duke Energy	Yes	
National Grid	Yes	
SPP Standards Review Group	Yes	
Ameren	Yes	
American Electric Power	Yes	
American Transmission Company, LLC	Yes	
Basin Electric Power Cooperative (BEPC)	Yes	

Organization	Yes or No	Question 3 Comment
California ISO	Yes	
Central Hudson Gas & Electric Corporation	Yes	
Clark Public Utilities	Yes	
Colorado Springs Utilities	Yes	
Edison Electric Institute	Yes	
Empire District Electric Company	Yes	
Exelon	Yes	
GridWise Alliance	Yes	
Independent Electricity System Operator	Yes	
ITC	Yes	
Minnkota Power Cooperative	Yes	
MISO	Yes	
Modesto Irrigation District	Yes	
Omaha Public Power District	Yes	
OPG	Yes	

Organization	Yes or No	Question 3 Comment
Pepco Holdings Inc.	Yes	
South Carolina Electric and Gas	Yes	
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	
The Empire District Electric Company	Yes	
The Empire District Electric Company	Yes	
Westar Energy	Yes	
California Public Utilities Commission: Safety and Enforcenment Division		In general, the overall method employed in the draft standard is reasonable. The draft standard has adopted a reasonable level of specificity, without being overly prescriptive.The use of unaffiliated verifying experts is a positive element in the draft standard. In general, we believe that the balancing authority or reliability coordinator for the transmission area in question is the best verifying expert. In the event the utilities disagree with the assessments of the unaffiliated verifying entities at any point in the process (for example see section 2.3, second bullet point), not only should the transmission owner or utility be required to document their technical rationale, but the standard should further delineate a process for resolving this disagreement. Section

Organization	Yes or No	Question 3 Comment
		5.1 of the draft refers to “resiliency”. Does this term refers to actions such as building redundancy or improving protective schemes, as opposed to direct physical protection activities? The standard should clarify the meaning of the term resiliency.Section 4.1 of the draft refers to “unique characteristics.” Assuming this consideration includes availability of spares and ease of repair, the language is acceptable.With respect to Rule 5, section 5.2, the drafting group should consider language requiring the security plan to include contact and coordinating information for other utilities or important stakeholders, in addition to law enforcement.With respect to Rule R6, section 6.4 the language requiring “non-disclosure” agreements is important and a positive element in the draft standard. Section 4.2 lists the elements to be considered in evaluating the potential threats and vulnerabilities to physical attack, and specifically states "[p]rior history or attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events and ...". We suggest that in additional to geographic proximity, that the section add language concerning "similarity of geographic characteristics". While geographic proximity, is a factor, ease of accessibility, layout and geographic contour, of an attacked facility is also important, if not more so.
ISO/RTO Standards Review Committee		The IRC has no comments on R4-R6.

4. **Do you have input on other areas of the standard or implementation plan not discussed in the questions above? If so, please provide them here, recognizing that you do not have to provide a response to all questions. Please limit your response to 300 words or less.**

Summary Consideration: The SDT appreciates all the additional comments submitted. All comments have been reviewed and changes that the SDT considers appropriate were incorporated into a subsequent revision. Several additions and clarifications were made to the Guidelines and Technical Basis section. A summary of comments and the SDT's response is provided. Note that some of the comments were previously addressed in preceding sections; the SDT's response is not repeated here.

- **Commenters suggested clarification of general terms including control center, primary control center, back-up control center, and widespread.** The SDT provided clarifications in the Guidelines and Technical Basis section.
- **A commenter recommended providing guidance for jointly owned substations.** The SDT has added commentary in the Guidelines and Technical Basis section to addresses joint ownership.
- **A commenter stated that the standard should explicitly allow a single plan to be developed to meet CIP-006 and CIP-014 requirements.** The SDT is aware that there may be a CIP-014-1 and CIP-006-5 physical security plan that differ, given that one is protecting against threats to cyber assets and another is protecting against physical threats. It is also aware the equipment and perimeters of protection will in many cases be significantly different between cyber assets being protected under CIP-006-5 and physical assets under CIP-014-1. Given these different purposes, the SDT believes it is appropriate to keep the physical security plans separate.
- **A commenter recommended providing clarification in the Guidelines and Technical Basis section to avoid placing risk on a verifier who is also a registered entity.** The SDT agrees that verifiers are not subject to violation of CIP-014-1. The plain language of CIP-014-1 in no way implicates that a verifier or reviewer, even if a registered entity, can be found in violation of CIP-014-1 for the work they do as a verifier or reviewer. Also, the language of Part 2.2 was revised to alleviate this concern.
- **A commenter suggested applying Cost Effectiveness Analysis Process (CEAP) to the standard.** The proposed Standard provides TOs and TOPs the ability to consider different methods to physically protect Transmission substations and stations and primary control centers implicated by this Standard. Therefore, the SDT believes that the application of CEAP is not needed.
- **Commenters proposed changing the implementation plan so that compliance with Requirement R1 would not occur simultaneously with the effective date of the standard.** The SDT considered alternate implementations but believes the proposed Implementation Plan provides entities sufficient time to complete Requirement R1 and strikes a balance between risk to the BPS and burden to the responsible entity.
- **A commenter recommended a SAR be developed to examine additional physical security issues and include additional entities in the physical security standards.** The SDT's scope is set forth in its SAR, and will work within that scope. The SDT considered and does not see the need to require the inclusion of RCs and BAs in the proposed Standard. Under the BA, EOP, IRO and TOP

standard families, RCs and BAs already have Real-time communication and oversight requirements, and the SDT does not see a need to duplicate those in CIP-014-1.

- Commenters provided editorial feedback on the VRF and VSL table that was accepted by the SDT where agreed.
- Commenters provided recommended changes to the RSAW which have been provided to the RSAW team.
- Commenters made suggestions regarding general readability of the standard; the SDT accepted recommendations where appropriate.

Organization	Yes or No	Question 4 Comment
FirstEnergy	No	FirstEnergy supports the proposed standard and appreciates the teams consideration of our comments intended to help clarify a few areas of the standard. FirstEnergy appreciates the team's efforts in producing a quality standard within an expeditious schedule and believes the team has provided a product that meets the core expectations described by the FERC Order.
ACES Standards Collaborators	No	Thank you for your time and consideration.
Ameren	No	We recommend adding language in the implementation guidance around the application of the terms 'control center', 'primary control center', and 'transmission station' in the draft standard.Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies' ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for carefulconsideration of various facts and circumstances that might inform content offormal NERC defined terms.Also, we recommend that the standard drafting team (SDT) consider additions or changes to theimplementation guidance that will clarify several questions on the timing of the various implementation stages of the standard, including particularly that security plans are subject to change over time for a broad

Organization	Yes or No	Question 4 Comment
		range of reasons. In addition, we ask the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work.
Duke Energy	Yes	(1) Duke Energy suggests that language should be incorporated either in the proposed standard or RSAW to allow for the flexibility in modifying the timeline specified in R5.3. We believe there are unforeseen circumstances that could occur which would result in the proposed timeline shifting from the intended completion date.Examples include, but are not limited to:a. Unplanned outage of transmission or generation facilities that results in canceling scheduled work.b. BES reliability concerns should the facility be out of service for a short or extended period of time.c. Third party vendor's availability in implementing recommendations made by an entity or unaffiliated third party verifier.For these reasons, we believe a provision is needed to allow for this type of flexibility in modifying the timeline specified in R5.3.
Manitoba Hydro	Yes	(1) R6.1 - It is not clear whether only one or all of the qualifications in Section 6.1.1 through 6.1.4 must be met. Accordingly, R6.1 should be rephrased to refer to "one of the following".
Utility Services	Yes	1 "primary control center" is confusing. NERC has a defined term "Control Center" which is intentionally not being used. What is the intent of not using the defined term? If the undefined term remains in use more clarity needs to be given on "primary control center".2. what is the definition of "widespread?" Does this mean outside of a Balancing Authority Area, outside of a Region or outside of an interconnection? More clarity is needed in the term. Additionally, TO's may not have the data required to perform this type of assessment. There needs to be process in place for the TOs to obtain the data required to perform the appropriate assessment. 3. The SDT should review projects such as PRC-006 or MOD C, and define groups within the requirements to reduce the length of requirements. For example R4 could be reduced to the following, making the requirement easier to read and adding much

Organization	Yes or No	Question 4 Comment
		needed clarity: “Each Applicable Entity shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Applicable Facilities as identified in R1 and verified in R2. The evaluation shall consider the following:... “RSAW Comment:R1 “Evidence Requested” section doesn’t provide a time frame for the first assessment, no assessment prior to effective date will be considered, but there must be an assessment completed before the effective date to be complaint. This is a catch 22.
MidAmerican Energy Holding Company	Yes	1. The standard anticipates the potential for joint responsibility in involving transmission operator control centers for substations identified by transmission owners. It is suggested that additional guidance be provided regarding joint ownership of substations The following addition to the first paragraph under the Requirement R1 heading which is similar to an aswer to this questions in the webinars is suggested: For substations that are jointly owned the owners may jointly designate one of the joint owners to perform the risk assessment for that substation. 2. It is suggested that a clarification be made to the RSAW with regard to the following question: “ As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?” By referring to risk assessment this seems to imply the stations/substations identified after the completion of the requirement R1 risk assessment rather than just the applicability requirements. It is suggested that the words “as a result of your risk assessment” be deleted from this question. 3. Item 3. in the guidance for Requirement R2 seems to actually be guidance for Requirement R1. However, it does not provide useful guidance for Requirement R1; therefore, it should be removed. The guidance for Requirement R1 that gives the TO discretion to choose its own methods and criteria is preferred.4. The following modification to one of the sentences in the “Performing Risk Assessment” section of the guidance document is suggested: “Using engineering judgment, the Transmission Owner should develop criteria (e.g. imposing a fault near

Organization	Yes or No	Question 4 Comment
		the removed substation) to identify a contingency resulting in potential widespread instability, uncontrolled separation or Cascading within an Interconnection."
American Public Power Association (APPA)	Yes	APPA supports approval of the proposed physical security standard, subject to the technical clarifications and corrections shown below. These comments were developed by APPA staff based on extensive input from a diverse group of members utilities that will be subject to the proposed standard once it is approved. Please see also the individual comments of APPA members.See comments on definitions under Question 1.RSAW for R1 poses the following question: "As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?" This question combines a multi-step process into a single question that cannot be answered as yes or no by many TOs. Please break the RSAW for R1 into three discrete questions:1...Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of 4.1.1?2...Have you conducted a risk assessment of each applicable station or substation identified under Applicability section 4.1.1.?3...Did the risk assessment identify one or more Transmission station(s) and/or Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection?RSAW R1 evidence request text from near the top of page 6: (R1) Provide the current and the immediately preceding risk assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant). The draft Implementation Plan states that the risk assessment required by R1 "must be completed on or before the effective date of the standard," yet the RSAW language provided above seems to exclude such an assessment.RSAW R1 "Note to Auditor" on page 7: "Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary." The text appears to reference the following question from page 6: "As a result of your risk assessment, do you own any Transmission stations/substations, either existing or planned in the next 24 months,

Organization	Yes or No	Question 4 Comment
		meeting the applicability requirements of 4.1.1?" This question is poorly worded, because TOs not meeting the applicability requirements of 4.1.1 are effectively exempt from this standard and do not need to perform a risk assessment.RSAW R3 "Question" on page 11: Please reword to add the following all caps text: "Are THERE any primary control centers identified in Requirement R1, Part 1.2 THAT ARE not under operational control of your NERC registration? RSAW R4 "Compliance Assessment Approach" on page 14: Change "or" to "OF" (R4 Part 4.2) "Prior history OF attack..." See the language used in the Guidelines and Technical Basis on page 31 of the standard.RSAW R5 "Note to Auditor" on page 16 states: "Auditor should cross reference the Transmission stations/substations and primary Control Centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities that would facilitate physical attacks that have a high probability or likelihood of occurrence." The requirements of the standard do not address "probability" or "likelihood" of occurrence, so these factors should not be in scope of the compliance audit. Rather, auditors should address whether the security plan is complete and the TO or TOP addresses the issues raised by the third-party reviewer.
American Transmission Company, LLC	Yes	ATC supports the draft standard, with the realization that the aggressive time line has raised a broad range of issues or ambiguities resulting from the use of vague language or generic terms. While ATC understands the necessity for this approach, given the compressed timeframe directed by the FERC Order, the project's condensed timeline may not have afforded for the necessary and careful consideration of these terms. Improved guidance around the application of generic terms would increase clarity and help the industry. ATC also supports a follow up effort commensurate with typical standards drafting processes and timeframes to allow for further consideration, improvement, and cleaner language to assure effective implementation of the standard. An example of language like this is in Requirement R1, which includes the vague terminology of "widespread instability, uncontrolled separation, or Cascading." Risk assessment findings can vary

Organization	Yes or No	Question 4 Comment
		significantly depending on the assumptions, criteria, and methodology used for the assessment, and a more thoughtful use of terms could provide for a more uniform risk assessment basis.
Encari	Yes	CIP-014-1 should expressly permit one well-coordinated physical security plan for a Transmission Facility. As proposed, there could be a separate physical security plan under CIP-006-5 for BES Cyber Systems within an applicable Transmission Facility and potentially another physical security plan for the Transmission Facility as whole under CIP-014-1.
Southern Company: Southern Company Services, Inc.;Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation and Energy Marketing	Yes	Clarification should be made in the implementation guidance for CIP-014-1 that Verifiers who are also Registered Entities in functions applicable to CIP-014, are not subject to penalty under the requirements of CIP-014 due to verification duties performed at the request of a responsible Transmission Owner and/or Operator.
Tampa Electric Company	Yes	Comments: Comments to DefinitionsTampa Electric also urges the SDT to define certain terms that appear in the standard: 1) “Transmission substation” and “Transmission station,” 2) “collector bus,” and 3)”primary control center. There terms are not defined in the NERC Glossary and may not have definitions that are universally accepted by the industry. “Transmission substation” and “Transmission station”Many industry practitioners use the term “Transmission substation” generally, whether or not any transformers are installed in the facility they are describing. Other practitioners apply the term “Transmission substation” only to facilities that include transformers. The standard implicitly uses the term “Transmission station” in reference to transmission switching arrangements that do not involve transformers. However, the more commonly used term for a transmission switching arrangement that does not include transformers is

Organization	Yes or No	Question 4 Comment
		"Transmission switchyard." NERC addressed this issue in the Guidelines and Technical Basis section of CIP-002-5. The SDT could easily carry that text over to the Guidelines and Technical Basis section of CIP-014-1. However, it would be better to add definitions for "Transmission substation" and "Transmission station" to the Glossary of Terms Used in NERC Reliability Standards. The relevant text in CIP-002-5 is copied below for the convenience of the SDT.CIP-002-5 Guidelines and Technical Basis clarifications of "Transmission stations" and "Transmission substations" The SDT uses the phrases "Transmission Facilities at a single station or substation" and "Transmission stations or substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist."Collector bus""Collector bus" is another term that is not defined in the NERC Glossary and that may not have a definition that is universally accepted by the industry. "Collector bus" appears in 4.1.1.1 and in 4.1.1.2. of CIP-014-1 in text that was carried over from CIP-002-5.4.1.1 Transmission Owner that owns any of the following:4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility. [Underlines added]4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a

Organization	Yes or No	Question 4 Comment
		Transmission Facility, but is part of the generation interconnection Facility. [Underlines added]If “Collector bus” is not defined or clarified, some TOs may conclude that some part of every transmission substation or switchyard that receives the output of a generator(s) is excluded from the scope of the standard. However, that is not the case nor the intent of the SDT. Therefore, the drafting team should consider whether it should define or clarify in the guidance document, the term “collector bus” “Primary control center”The NERC Glossary defines “Control Center” in this manner:One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.What might not be clear for the purposes of CIP-014-1 is what exactly distinguishes a “primary control center” from other alternate “Control Centers.” Some registered entities can operate substations from multiple locations. Often, there is one self-designated “main control center” or “primary control center” for which there might be multiple alternate or “backup control centers.” Given that alternate or backup control centers have capabilities that are comparable to so-called main control centers, it might not be clear in some systems whether “primary control center” in CIP-014-1 applies to more than one Control Center.The SDT can solve this problem by adding a definition of “primary control center” to the NERC Glossary or by adding text to CIP-014 that for each critical substation the TO or TOP can designate any Control Center as the “primary control center.”
Pacific Gas and Electric Company	Yes	Compliance 1.2 (pg. 13) Comment: can they clarify by being less wordy and just start by saying “The responsible entities shall retain documentation as evidence for three years”, followed by the rest in less words?
Public Utitliy District No. 1 of Cowlitz County, WA	Yes	Cowlitz commends the SDT's effort in a very difficult situation.

Organization	Yes or No	Question 4 Comment
Ciy of Garland	Yes	Definitions:primary control center - although not capitalized and therefore not a defined term, it is used in this standard in requirements 1, 3, 4, 5, and 6. The same term "primary control center" (again not capitalized) is used with a completely different meaning in standards EOP-008 in requirements 1.3, 1.5, 1.6, 2, 3, 4 and 7.1. Similarly "primary control room" is used in EOP-005 requirement 5 and in EOP-006 requirement 6 and is defined as the control center from which a TOP normally operates as opposed to the backup center. In CIP-014, it is defined/implied to be the control center that actually controls the circuit breakers at two or more substations. o If the term “primary control center” is used there will be confusion over the different meanings within the NERC Reliability Standards. o A completely different term should be used such as “primary local control center” or “primary transmission operations center”. The SDT apparently meant a "facility that has direct Supervisory Control". The term should be defined completely in the standard and should become a defined term within the Glossary of Terms used in NERC Reliability Standards. Proposed defined term:Primary Transmission Operations Center - One or more Transmission Owner or Transmission Operator facilities hosting operations personnel having primary operational real-time control of the BES elements in one or more remotely located substations using SCADA, EMS or other electronic means.”Please clarify whether these security plans are also required at any backup control center. Many of these control centers are generally not manned on a 24 by basis.unaffiliated - should be either defined or a footnote needs to be added to the Standard to explain that unaffiliated - means the selected verifying or reviewing entity cannot be a corporate affiliate, as stated in the guidance document. o Would two entities that do not have a direct ownership stake in each other but both are parties to an ownership in a third organization be considered to be unaffiliated? Example: Two utilities each have an ownership of a joint power plant but no ownership of each other. o What if they both had no ownership of the third party but both had purchase contracts with a third party? An explanation needs to be in the standard and not in the separate guidance document.

Organization	Yes or No	Question 4 Comment
Consumers Energy Company	Yes	Develop a requirement to protect information shared between entities and third party organizations. Requirement number 6 should be revised to state "...third party reviewer that is either..." 6.1.1 or 6.1.2 or 6.1.3 or 6.1.4. R6 seems vague and should be revised
Edison Electric Institute	Yes	EEI supports the draft standard CIP-014-1 as fully responsive to the FERC March 7 order. The project has moved along a very aggressive timeline and naturally raises a broad range of practical and implementation issues. Based on extensive discussions with member companies, EEI recommends that the standard drafting team (SDT) consider additions or changes to the implementation guidance that will clarify for companies several questions on the timing of the various implementation stages of the standard, including especially that security plans are subject to change over time for a broad range of reasons. In addition, EEI asks the SDT to consider clarifications in implementation guidance that, in many cases, the completion of all mitigation work may take place on longer timelines, and that implementation of a security plan does not require the completion of all mitigation work.Observing the many meetings and webinars that have taken place recently, EEI also recommends that the SDT consider adding language in the implementation guidance around the application of the terms 'control center,' 'primary control center,' and 'transmission station' in the draft standard. Obviously, there are a wide variety of understandings on these terms and additional clarity will help companies' ability to perform under the requirements. Considering that these terms have generic application to bulk power system reliability, the project timeline does not afford time for careful consideration of various facts and circumstances that might inform content of formal NERC defined terms.
SPP Standards Review Group	Yes	Effective Date:The use of the term 'implement' needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the

Organization	Yes or No	Question 4 Comment
		drafting team. VSLs:Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2.Insert 'and verified according to Requirement 2' following the reference to Requirement R1 in all the VSLs for R5.Delete 'and modify or' in the last High VSL for R6.Guidelines and Technical Basis:Replace 'drafting team' with 'SDT' in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6.Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary.Insert 'Transmission', capitalize 'Owner' and delete 'or operator' in the 1st paragraph under Requirement R2 on Page 29.Make 'outage' plural in Bullet c. at the top of Page 30.Capitalize 'Transmission Owner' in the 4th bullet in the middle of Page 30.Capitalize 'Owner' in the 1st line of the paragraph immediately preceeding Requirement R3.Insert 'Requirement' in front of R5 in the last line of the paragraph immediately preceeding Requirement R6.Spell out TO and TOP throughout the document. RSAW:The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states '...any risk assessments conducted prior to the effective date of this standard are not relevant...' is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there 'This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.' We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states "The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard." Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective.Replace 'with' with 'within' in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2.Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4.The phrase 'and compensating mitigating

Organization	Yes or No	Question 4 Comment
		measures' in the 4th row in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Westar Energy	Yes	Effective Date:The use of the term 'implement' needs clarification . To some implement means installed and in-service. To others it could mean a work in progress. The SDT recognized this confusion in the webinars on April 17 and we encourage them to modify the language to more clearly indicate the intent of the drafting team. VSLs:Capitalize Part 2.3 in the Lower, Moderate and High VSLs for R2.Insert 'and verified according to Requirement 2' following the reference to Requirement R1 in all the VSLs for R5.Delete 'and modify or' in the last High VSL for R6.Guidelines and Technical Basis:Replace 'drafting team' with 'SDT' in the last paragraph under Section 4 Applicability on Page 27. Make the same change in the last paragraph on Page 32 under Requirment R6.Capitalize Remedial Action Schemes (RAS) and Special Protection Systems (SPS) in the paragraph at the top of Page 29. These are defined terms in the Glossary.Insert 'Transmission', capitalize 'Owner' and delete 'or operator' in the 1st paragraph under Requirement R2 on Page 29.Make 'outage' plural in Bullet c. at the top of Page 30.Capitalize 'Transmission Owner' in the 4th bullet in the middle of Page 30.Capitalize 'Owner' in the 1st line of the paragraph immediately preceeding Requirement R3.Insert 'Requirement' in front of R5 in the last line of the paragraph immediately preceeding Requirement R6.Spell out TO and TOP throughout the document. RSAW:The parenthetical statement in the 1st row of the table under Evidence Requested for R1 that states '...any risk assessments conducted prior to the effective date of this standard are not relevant...' is inconsistent with the statement on the Consideration of Issue or Directive in response to paragraph 12 of the FERC order. It states there 'This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard.' We believe the latter is consistent with the view expressed by SDT members on the two webinars conducted on April 17. This is also inconsistent with the posted Implementation Plan in which it states "The initial risk

Organization	Yes or No	Question 4 Comment
		assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard." Additionally, this is inconsistent with others standards in that action is sometimes taken prior to the effective date of the standard in order to be compliant when the standard becomes effective.Replace 'with' with 'within' in the 3rd row of the table under Compliance Assessment Approach Specific to CIP-014-1, R2. This is the row for R2, Part 2.2.Use lower case control center in the Note to Auditor box at the bottom of the table under Compliance Assessment Approach Specific to CIP-014-1, R4.The phrase 'and compensating mitigating measures' in the 4th row in the table under Evidence Requested for R6 goes beyond the requirement in the standard. The requirement only calls for the reasons for not modifying the security plan according to the reviewer recommendations. It doesn't require the Responsible Entity to specify how it will mitigate the discrepancy.
Florida Municipal Power Agency	Yes	FMPA has concerns for the RSAW and the lack of direction to auditors from the RSAW concerning the scope of their review. The auditor should not have a subjective decision regarding the sufficiency of the risk assessment, vulnerability assessment or security plan of the TO/TOP. The unaffiliated 3rd party is the source of qualified expert subjective opinion on the sufficiency of the risk assessment, vulnerability assessment and security plan. As such, the RSAW ought to clearly define the scope of the auditor's review of the risk assessment, vulnerability assessment and security plan. FMPA suggests rewording the "Compliance Assessment Approach"portions of the RSAW that call for these reviews to read something like the following (specific to R1):Review the entity's risk assessment to answer the following:a. Were all of the entity's assets, existing and planned to be in service within 24 months of the date of the documented risk assessment, and applicable to the standard (Applicability Section 4.1.1), included in the assessment?b. Was a transmission analysis or transmission analyses identified and documented to evaluate whether any applicable Transmission station(s) and Transmission substation(s), if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection? The auditor is not to evaluate the sufficiency of such analyses; but rather whether such analysis was documented.c. Was the assessment

Organization	Yes or No	Question 4 Comment
		conducted within the timeframes identified in bullet 1.1?d. Was the primary control center(s) identified in accordance with bullet 1.2?
Public Utility District No. 2 of Grant County, WA	Yes	GCPD feels that the implementation schedule is somewhat arbitrary and demonstating compliance with the implementation schedule conflicts with language contained in the proposed RSAW.GCPD supports RSAW edits as proposed by APPA to address these discrepancies.GCPD proposes the following edits to Requirement language addressing implementation timing to allow for enforceable and auditable time lines not dependent upon the unique completion date of the initial risk assessments conducted by the RE.2.2. ...The Transmission Owner shall ensure the verification of the initial risk assessment performed under Requirement R1 is completed within 90 calendar days following the effective date of this Standard.Subsequent risk assessments shall have verifications completed within 90 calendars days of completion of the risk assessment.R5. ...and primary Control Center(s) within 210 calendar days following the effective date of this Standard. Changes to recognized applicable facilities under this Standard as identified under Requirement R1 and verified according to Requirement R2, shall require review of the physical security plan(s) within 90 calendar days of completion of associated risk assessments. ...General commentary: in October 2012 the Cost Effective Analysis Process (CEAP) was approved for a “pilot”. The NERC CEAP was intended to integrate cost consideration and effectiveness into the development of new and revised standards. The first phase of the CEAP was to be implemented during the SAR stage to determine cost impact and identify “order of magnitude” or potentially egregious costs, to determine if a proposed standard will meet or exceed an adequate level of reliability, and what potential risks are being mitigated. The second phase was to be conducted later in the standard development process and afford the industry the opportunity to offer more cost efficient solutions that may be equally effective to achieving the reliability intent of the draft standard. This report would be posted at the time the standard is balloted. The report was intended to present the data collected in a manner which will provide the industry with representative cost implementation and effectiveness information to allow a more informed choice

Organization	Yes or No	Question 4 Comment
		during balloting. Based upon the urgent nature of this Standard, phase two would need to be applied. The CIP-014 Standard requires costs to be incurred to comply with Requirement R5. In addition, there may be substantial costs incurred to implement the Physicial Security Plan(s). The CIP-014 Standard is an ideal standard upon which to exercise the CEAP. The information resulting from the CEAP would be beneficial not only to government officials, but also the industry as a whole.
Georgia System Operations Corporation	Yes	GSOC supports the comments submitted by NRECA
Georgia Transmission Corporation	Yes	-GTC supports the comments submitted by the NRECA with regard to the applicability, requirements, and implementation of the draft standard.-GTC suggests that in M2 the word “communications” be changed to “notifications” to follow the language of t
GridWise Alliance	Yes	GWA includes electric utilities, information and communications technology service and equipment providers, Independent System Operators (ISOs) and Regional Transmission Organizations (RTOs), academic institutions, and energy consulting firms. GWA appreciates the acknowledgment in the Order of the significant efforts that industry already is undertaking to enhance the resilience of the electric grid and thereby protect the grid from a range of threats, including physical, cyber, natural, and other hazards. Industry has been working in close partnership with various levels of government to enhance grid protection, reliability, resilience, and security. This collaboration is ongoing and should be fostered for the future.As you are aware, the electric grid is dynamic in nature. Electric grid owners and operators are making investments to enhance the reliability and resiliency of the grid, and are actively managing the operation of the grid to prevent outages and to restore power expeditiously, when outages do occur. As this process moves forward, GWA wants to underscore the importance that the result not be overly burdensome or inhibit innovation. It is important that the risk assessment process indeed be limited to truly “critical” infrastructure that is deemed essential to the functioning of the bulk electric

Organization	Yes or No	Question 4 Comment
		system. This will help ensure that protection measures are reasonable and cost-effective, as well as cost-sensitive, to help minimize costs to industry and also to consumers, who ultimately must bear the costs of these investments. Industry is working hard to monitor and stay ahead of the myriad threats that could arise - physical, natural, cyber, and otherwise - recognizing that the types of threats and the motivations of potential actors continue to change over time. NERC should partner with FERC to ensure that an all-hazards approach to addressing risk is undertaken going forward. We appreciate the Order's acknowledgement of the vital need to protect confidential and sensitive information. Yet, we are concerned about the nature of information-sharing under this Order, and what protections and assurances, in fact, would be implemented to prevent the inappropriate sharing of confidential information. While also recognizing the need to protect the confidentiality of such sensitive information, we also note that it is important to ensure that information sharing is facilitated between the government and the private sector, as well as within the private sector. Vendors who supply critical systems and equipment are incorporated into this process, since continued coordination and cooperation among all the stakeholders is essential.
Rayburn Country Electric Cooperative	Yes	I think the standard IF broken up into 2 standards (High, Med) should provide clearer guidance as to the expectations of the plans content. Similar to the issues that arose with the Low assets in CIP V5 . Give basic structure and content to be addressed to give FERC the assurance the specific concerns have been met.
Minnkota Power Cooperative	Yes	In the "Draft_RSAW_CIP-014-1_v1_2014_0409.pdf" document, on page 4 of 22, there is a Note to Auditors Concerning Third Party Verifications and Reviews. In this section there is a mention to the "concept of reliance means using the work of others to avoid duplication of efforts". While the reference to "duplication" was in regards to unaffiliated third party verifications and reviews, we appreciate the SDT be congnitive of "duplication of efforts" as their developing the Standard and the RSAW. With the very restrictive timeframe for which the development of the Standard was required, this concept can get lost. We did see another area in the Standard CIP-014-1 R5.2,

Organization	Yes or No	Question 4 Comment
		which may be considered “duplication of efforts”. CIP-014-1 R5.2 states, the TO/TOP should have in their physical security plan(s) law enforcement contact and coordination information. On June 20, 2013, FERC approved Reliability Standard EOP-004-2, which identified types of reportable events and thresholds for reporting, requires responsible entities to have an operating plan for reporting applicable events to NERC and other entities (including law enforcement), and requires reporting of threshold events with a 24 hour period (Docket No. RD13-3-000). This Standard covers the need to incorporate law enforcement contacts in the operating plan. Requesting this type of information in both the operating plan required in EOP-004-2 and physical security plan in CIP-014-1 is a “duplication of efforts”. MPC believes the intent for CIP-014-1 was to identify and mitigate physical security risks, while the intent for EOP-004-2 is to improve reliability of the BES by requiring the reporting of events by Responsible Entities. MPC suggests removing Requirement 5.2 in CIP-014-1.
Western Area Power Administration	Yes	In the VSL for requirement R5, in all four severity levels, states that the security plans need to be developed for the facilities “identified in requirement R1”. However Requirement R5 only requires the plans to be developed for facilities ‘identified in Requirement R1 and verified according to Requirement R2,”. The VSL should be modified to include the statement ‘and verified according to Requirement R2.The first row in the Table, in the RSAW, describing the evidence required in requirement R1, it states that any risk assessments conducted prior to the effective date of this standard are not relevant. The Implementation Plan states that “The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard.” There appears to be a conflict between these two statements, unless the intent is that the initial risk assessment needs to be completed on the effective date. Also, normally, unless the implementation plan provides a different time line, you need to be compliant by the effective date.In the RSAW for requirement R6 the fourth row in the Evidence Requested table, it asks for evidence that includes the “reasons or compensating mitigating measures for not implementing the recommendations for the reviewing party.” Requirement R6.3 of

Organization	Yes or No	Question 4 Comment
		the standard only requires the Transmission Owner or Transmission Operator to "Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation." These two statements should be clarified in order to ensure consistent enforcement.
American Electric Power	Yes	It is AEP's understanding that regarding R5, the phrase "develop and implement a documented physical security plan...within 120 calendar days" means that, within 120 days, the physical security plan must be completed and that the entity is working toward implementing the plan and does not mean that the plan must be fully implemented within 120 days. AEP urges the clarification of that expectation within R5 so that the requirement is unambiguous. Regarding R6.4, please clarify whether the procedures for protecting sensitive or confidential information would include suitable terms and conditions within a third party contract.
Northeast Power Coordinating Council	Yes	It is NPCC's expectation that RAI concepts will be applied to the operating and enforcement of this standard.
Omaha Public Power District	Yes	OPPD believes that the third-party verifications in requirements R2 and R6, to be performed once every 60 calendar months, not each time when a risk assessment analysis or security plan is changed that does not significantly change the facilities identified or the associated security plan. The transmission entity can still perform analysis and update security plan accordingly as required by this standard, however, the third-party verification should be reserved for major changes to the assessment or the plan or otherwise be done every 60 calender months.
Lincoln Electric System	Yes	R1 - It appears the intent of R1 is for a TO (which meets the applicability section 4.1.1) to perform a risk assessment (as defined in the standard) on only those substations that meet the applicability section 4.1.1, not all substations owned by a TO which meets the applicability section 4.1.1 description; however this is not 100% clear. The verbiage of the second sentence in R1 states "The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses

Organization	Yes or No	Question 4 Comment
		designed to identify any Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection." The use of the word "any" in this sentence has led some to believe that a TO (which meets the applicability section 4.1.1 description) will have to assess all of their substations, even those that do not meet the section 4.1.1 description. To address this possible issue, LES recommends replacing the word "any" in R1 with "applicable".R2 - Smaller TOs may not have the in-house resources to perform the risks assessments required in R1, and may need to contract with a third party to perform these assessments. If the performing third party is not affiliated with the TO, is a second unaffiliated third party verification required as stated in R2? Please revise the requirement to address this situation.
Bureau of Reclamation	Yes	Reclamation is concerned that the term "primary control center" will become confused with the NERC Glossary term "Control Center." As indicated by the use of the term "monitor" in the definition of Control Center, Reclamation does not believe that the concept of "operational control" has been equated with "causing direct physical action" to date. To avoid confusion, Reclamation suggests that the drafting team replace the R1 phrase "primary control center that operationally controls eachTransmission station or Transmission substation" with the phrase "primary control center that physically controls each Transmission station or Transmission substation."
City of Garland	Yes	Recommendation # 1 - Include the timeline diagram located in the FAQ document titled "CIP-014 Physical Security Process Flow" in the Guideline and Technical Basis section of the standard. This diagram clearly demonstrates the timing between the different requirements. Because of the subsequent risk analysis's in R1, verifications in R2, and potentially the processes outlined in R3, R4, R5, & R6, questions on timing (answered by the diagram) potentially will arise throughout the life of the standard. Recommendation # 2 - Add the words "catastrophic failure" to the Purpose statement. On a webinar, there was discussion concerning the Purpose statement and it was stated a number of times that "widespread instability, uncontrolled

Organization	Yes or No	Question 4 Comment
		separation" meant to convey the concept of "catastrophic" - there will be a lot of folks involved in the implementation of the standard who did not hear the webinar comments.Recommendation # 3 - Rather than the term "primary control center" used in all the proposed requirements, use a different term or phrase such as the "facility that has direct Supervisory Control". The word "direct" in the recommendation of "direct Supervisory Control" should replace the need for the word "primary" - primary makes one think of primary and backup (which is not addressed in the standard). The concern with using primary control center, even though "control center" is not capitalized, brings up a mental picture of primary (and backup) Control Centers as defined in the NERC glossary. The standard should be straight forward, not using terms that can be confused.
Seattle City Light	Yes	Seattle City Light supports the Question 4 comments of APPA.
Salt River Project	Yes	Section C "Compliance" 1.4 (page 13) which states "...all evidence will be retained at the TO and TOP facilities." is contradictory with NERC Compliance Monitoring and Enforcement practices which allow data to be exchanged with and sent to Regional Entities such as in pre-Audit data requests and Mitigation Plans. In addition, this would be burdensome for the TO/TOP because the 3rd party verifying/reviewing entities would need to be on-site and potentially incur travel expense.
Con Edison and Orange & Rockland	Yes	Section: PurposeComment: Use of term "primary control center" should be clarified. If an entity has a primary control center and a redundant back up control center, is the back up control center also in scope for CIP-014? Requirement 1: is the intent of the Standard that the R1 risk assessment be applied to transmission stations or substations identified under Applicability 4.1.1.4, as meeting NPIRs? Requirement 4: If under Requirement R4 a Transmission Owner owns or operates a single substation that employs multiple voltage levels, then which portions of that substation would be covered by CIP-014-1 and the Entity's physical security plan, and which would not be covered? Requirement 5: Consideration of transmission system "resiliency" is more

Organization	Yes or No	Question 4 Comment
		appropriate to be applied during the R1 risk assessment, as opposed to the R5 physical security plan. Recommend moving references to resiliency to R1.
Texas RE	Yes	Several places in the standard refer to notifying the Transmission Operator for stations that meet the higher risk profiles. However, the language is not clear as to what is expected from the Transmission Operators when a physical security incident occurs at one of those substations during real-time operations. Finally, this entire process can exceed four hundred days, which is excessive.
Xcel Energy	Yes	Since existing criteria from CIP-002-5.1 is used to identify facilities in scope, Xcel Energy suggests the addition of the proposed requirements be incorporated to CIP-006-5 (rather than in an entirely new standard) to more closely align and standardize the oversight of R3 and R6. In addition, this would centralize all physical security requirements within a single Standard. Additionally, there is a significant amount of language in the requirements to specify the affected parties. We suggest the Standard Drafting Team seek opportunities to more concisely outline the applicability and the subsequent obligations in the requirements, to improve ease of understanding. We see an opportunity for the audit or risk functions of the Regional Entities to align with the third party review criteria established in the proposed standard. Although the expertise to perform this function may not currently be in place, the Regional Entities could easily develop the knowledge and expertise, and the reviews could naturally integrate within their other review and assessment activities.Overall, the standard is very comprehensive as drafted and it is balanced in a manner that allows for maximum flexibility. Consistent with NERC's evolution to results-based standards, it is appropriate for the standard to focus on the desired results of increased security of critical facilities, rather than mandating rigid actions that may or may not be suitable for individual facilities and entities. Allowing industry the latitude to design its own mitigating measures ensures those measures will be the most practical and cost effective as appropriate for the particular nature of each facility. The flexibility of this proposed standard is the best opportunity for the industry to execute a comprehensive solution based on assessments and security

Organization	Yes or No	Question 4 Comment
		that relies on the unique design and characteristics of the operating systems of each utility.
Nebraska Public Power District	Yes	Since we are using CIP-002-5 for identifying Transmission stations and substations, the confidential information for these facilities is already protected under CIP-011-1 Information Protection. CIP-014-1, requirements 2.4 and 6.4 are redundant with already approved requirements and are not needed. Adding requirements for protecting sensitive or confidential information in this standard will create confusion and double jeopardy. CIP-006-5 covers physical security and any information pertaining to the substations identified through the CIP-002-5 criteria. CIP-011-1 already protects this information.Due to the expedited development of this standard, sufficient time isn't available to provide clear requirements in the standard to evaluate compliance. The RSAW does contain language that will help, but the RSAW isn't the enforceable document and can be changed without industry approval. We've learned from implementing the other CIP standards that auditors can take a completely different position than what was meant by the drafting team with little recourse for utilities.
Southwest Power Pool Regional Entity	Yes	SPPRE recommends that subsequent risk assessments should be peformed at least every 36 calendar months regardless of whether previous risk assessments had identified critical facilities. It is more important to identify facilities that should be on the list than those that might not need to be on the list anymore.
PNM Resources	Yes	Support the comments submitted by EEI
Bonneville Power Administration	Yes	The current draft requiring "unaffiliated" third party review is more restrictive than the requirements language in the FERC order and meeting an unaffiliated requirement will be problematic for federally owned power and transmission systems. Paragraph 8 of the order: "Thus, the Reliability Standards should require the owners or operator to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically

Organization	Yes or No	Question 4 Comment
		contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process." BPA's interpretation of the FERC order is that consultation with peer entities would be acceptable methods for review of evaluation processes. In fact the order by its wording encourages such consultations without restriction as to business or corporate relationships. The draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The "unaffiliated" requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term "unaffiliated" and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard.Paragraph 11 of the FERC order: "In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity." BPA believes the draft standard limits and excludes highly qualified security and technical expertise found across the industry and within entities corporate and governmental structures, hierarchies and partnerships where vast levels of experience, training and ability exist. The "unaffiliated" requirement forces entities to seek expertise where there may or may not be such expertise and where there is no track record of such expertise. The term "unaffiliated" and any reference to that level of separation between entities are completely void from the order and should be removed from the draft standard.
Hydro QuÃ©bec TransÃ‰nergie	Yes	The following are suggestions to facilitate reading of the standard, as well as its future translation: All requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary.R1: Remove "transmission analysis" from the sentence "The initial and subsequent risk assessments shall consist of

Organization	Yes or No	Question 4 Comment
		transmission analysis or transmission analyses designed to ..." We believe this repetition is unnecessary.R2.2: The first part applies to an entity that is not subject to the standard and should be removed from the standard.R2.3: Replace the word "identification" with "assessment". Remove the word "either"Rephrase R4, R5 and R6 (add "a"): " ...a transmission substation, or a primary control center".R4 and R5: Remove the part "...that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation". It only complicates the reading of the requirement (the TOP is not notified by the TO unless it has operational control over an asset identified in R1). If the first parts of R4, R5 and R6 are intended to identify the functional entities to which the requirement applies, we suggest "... and each Transmission Operator notified by a Transmission Owner under requirement R3, shall ..." for the TOP portion (line 3 to 6 of R4, R5 and R6). We believe that it would greatly improve clarity and readability of the requirements.R6.1: rephrase to "from one of the following". Furthermore, the numbers 6.1.1 to 6.1.4 should be replaced with bullets as is the case in R1.1, R2.1, and R2.2. Rephrase R6.1 and R6.1.1 to reflect the language used in the rationale. We believe limiting the reviewer to someone with a CPP or PSP certification goes beyond what the FERC order requesting. Suggest rephrasing to "with appropriate expertise of the evaluation performed".Guidelines and Technical Basis on requirement R1: HQT agrees with the fact that the TO has discretion to choose the specific method to establish the risk assessment, and that it is relevant that the Guidelines proposes examples. However, the proposed example of "removing all lines to a single Transmission station" seems to present a very stringent impact considering a physical attack on a facility. We ask the SDT to propose others less stringent examples that would be more in line with realistic physical attack, such as loss of a large section according to physical organisation of the facility, or loss of all main transformers, etc.
NCPA Compliance Management Operating Committee	Yes	The Implementation Plan is too agressive. I cite NCPA experience as described in our response to question 2. I find it interesting the the CIP-version 5 standards have

Organization	Yes or No	Question 4 Comment
		essentially a two year implementation plan for medium and high assets and yet this proposed standard has a 6 month implementation plan.
David Kiguel	Yes	The Implementation Plan obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. While performing and completing the vulnerability assessment before the effective date of the standard may constitute a recommended good practice, from a statutory perspective, compliance with the standard before its effective date may not be enforceable in all jurisdictions. An entity cannot be found in violation of the standard at a time when the standard is not yet effective. Recommend changing the implementation plan to require completion of the assessment after the effective date of the standard.
South Carolina Electric and Gas	Yes	The requirement for unaffiliated third party verification throughout this standard is not consistent with other NERC Reliability Standard verification requirements. SCE&G is concerned that this standard sets precedence for future standard third party verification which would be very costly, confusing and burdensome.
Basin Electric Power Cooperative (BEPC)	Yes	The SDT should be applauded for the diligent work performed in short order to meet the requirements of the FERC order RD14-6-000 while allowing flexibility in the manner the Registered Entity may be compliant.
Idaho Power Co.	Yes	There is great concern related to information protection related to turning over information concerning vulnerabilities of the grid and related facilities to outside parties. Even with the use of NDAs, these third parties are not subject to the same NERC reliability standards (i.e. CIP standards, information protection, etc) as the entities, will not be audited on their information protection practices, and may have no accountability to the regulators in the event of a disclosure of sensitive information, inadvertent or otherwise. It is a concern that the TO is responsible for 3rd party verification to be completed within a tight 90 day window, especially considering the critical infrastructure information being exchanged. Contractual

Organization	Yes or No	Question 4 Comment
		exchanges and negotiations could impede upon the 90 day window. Also, TO's may need time to review the R2 study results and possibly mitigate study discrepancies. The date R1 needs to be performed is unclear. Does it need to be performed within a certain amount of time after the effective date? The implementation plan states that the initial risk assessment must be performed on or before the effective date of the standard. However, the RSAW for R1 states that "any risk assessments conducted prior to the effective date of this standard are not relevant." Does this mean the initial risk assessment must be performed “on” the actual effective date of the standard? Is there a basis for the short notification window in R3? The seven calendar days window for the TO to notify the TOP seems quite short. Additionally, there is a discrepancy in the review timeframes in R1 in which a look ahead of 24 months is required for stations and substations that are in the planning process but the risk assessments are performed every 30 months leaving a 6 month gap in the analysis. It would also seem more intuitive and consistent with other CIP standards to have the risk assessment requirement performed on an even year rather than a 30 month basis (i.e. 36 months.)
Pepco Holdings Inc.	Yes	There seems to be a conflict between the RSAW, Consideration of Issues or Directives and the Timeline included in the FAQ. To meet the overall timeline for the entire standard, the risk assessment must be started prior to the Effective date of the standard. There should be no prohibition for completion of the Risk Assessment prior to the Effective date of the standard.The FAQ Timeline states:”Initial performance of R1 must be complete on or before the effective date of the standard...”The Consideration of Issues or Directives #12: “...This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard...”The RSAW under R1 Evidence Requested states: “Provide the current and the immediately preceding risk

Organization	Yes or No	Question 4 Comment
		assessments conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant)."
EF Cass Consulting Inc.	Yes	This standard has the perceived importance of protecting national security and being so critical as to expedite its development through modification of nearly all associated controls. I agree physical security of critical facilities is of paramount concern but not at the expense of producing a sound standard. After listening to two of the webinars it is clear to me that the majority of the entities responsible for ultimately complying with this standard and those that will enforce the requirements are unclear as to what is required. I would suggest running it past the "Experts" for their review prior to the first vote.
ITC	Yes	Transmission systems tend to have facilities for which inoperability, while not causing immediate system failure or separation, would nonetheless leave the system in a degraded state. This degraded state will require system operators to reconfigure the system in a way to mitigate the loss of such facilities, but at that point, a new group of facilities could effectively become "critical" as that term is currently defined in CIP-014-1. For example, the loss of a given substation may cause several transformers to be inoperable, and with the long lead time for replacement components, the transmission owner would realistically need to plan for the substation to be out of service for an extended period of time. During this time in which the substation is out of service, a second tier of assets may exist for which inoperability would now cause separation or failure of the type that would afford them a "critical" designation as currently defined under CIP-014-1. This condition would persist for as long as the original equipment was out of service. If the SDT were to adopt ITC's proposed modifications to R1 (see above), this would not be an issue, since all CIP-002-5 substations would already be covered by CIP-014-1. However, if the SDT chooses not to adopt ITC's proposal, the SDT should consider whether entities should assess the transmission system in this new degraded condition to determine if new critical assets are created due to the degraded condition (i.e., a reapplication of the analysis performed in the current R1 to determine if the loss of a particular substation causes

Organization	Yes or No	Question 4 Comment
		widespread cascading.) The Standard could also trigger additional transmission system studies to determine if the transmission system remains reliable during the extended period in which the critical assets remain out of service.
Florida Keys Electric Cooperative	Yes	Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.
National Rural Electric Cooperative Association (NRECA)	Yes	Under the implementation plan for R1, how can compliance with a standard be required prior to the effective date of the standard? The drafting team should reconsider this element of the implementation plan. If included in future drafts, a legal opinion from the NERC General Counsel should accompany this issue for stakeholder consideration.
SERC CIPC	Yes	Until the process of the standards has more fully matured there should not be a presecribed methodology for conducting the Security Vulnerability Assesments (SVAs) as long as generally accepted criteria as well as as stated in the standard in 4.1, 4.2, and 4.3 are followed in the development of the evaluation and plan(s).The comments expressed herein represent a consensus of the views of the above named members of the SERC CIPC only and should not be construed as the position of the SERC Reliability Corporation, or its board or its officers.
Southern Indiana Gas & Electric Company d/b/a Vectren Energy Delivery of Indiana, Inc.	Yes	Vectren recognizes that this drafting effort required significant contraction of drafting and approval processes, and Vectren appreciates the work of the drafting team. Vectren is supportive of the goals of the standard, supports R1, R3, R4 and R5. Vectren urges the drafting team, NERC and FERC to remove entirely or add detail to the requirements R2 and R6, and to add specific audit criteria in the RSAWs, so that

Organization	Yes or No	Question 4 Comment
		entities can have some confidence that their risk assessments performed in good faith, will be considered compliant with this Standard.
Foundation for Resilient Societies	Yes	We recognize that FERC has established a 90-day review process, and that NERC has worked to meet the tight deadline. Hence, the Foundation for Resilient Societies asks NERC to develop a SAR for Physical Security Standards - Phase 2. In this process, analytical modeling should be undertaken to identify and prioritize physical security risks that include cyber vulnerabilities, and that relate to the need for reliable warning and communications via redundant channels to control centers and to law enforcement. It should not be acceptable to exclude Regional Coordinators and Balancing Authorities, both groups needing to review and perhaps upgrade their own physical security, and both groups playing key roles in oversight of the operating entities, both TOs and GOs, whose physical security may be essential to prevent long-term outages through coordinated attacks. For additional materials prepared by the Foundation for Resilient Societies, contact the FERC staff designated to assist NERC with standard setting in FERC Docket RD14-6-000.
PPL NERC Registered Affiliates	Yes	We recommend that the SDT include a timeline within the standard which includes all required steps.
Cooper Compliance Corp	Yes	We would like to address proposed comments by APPA that additional Standards are added to address confidentiality. We do not agree with APPA's position. The functional model requires registered functions to work together to secure reliability. Already, as a result of CIP Standards, vital communications between the Distribution Providers/Load Serving Entities and the Balancing Authorities and/or Transmission Operators have been compromised. Often, The Balancing Authorities and Transmission Operators are in fear of sharing important information with the Distribution Providers and/or Load Serving Entities because they feel they could be subject to a CIP violation. In some cases the Distribution Providers and Transmission Operators even share facilities. Having a requirement that prevents sharing vital

Organization	Yes or No	Question 4 Comment
		information on physical security would simply not work and therefore we do not support APPA's comments.
Western Electricity Coordinating Council	Yes	WECC believes that the proposed standard addresses the FERC Order and has voted affirmative to approve CIP-014-1. However, as noted in our comments above we believe there is opportunity for enhancements and clarification that if implemented would improve the standard and still meet the FERC Order. WECC encourages the drafting team to consider implementation of these suggestions prior to the final ballot or NERC to submit a SAR for consideration of these suggestions immediately after approval of the standard.
Tri-State Generation and Transmission Association, Inc.	Yes	While the FERC Order RD14-6 paragraph 13 does require NERC to file a proposed standard within 90 days, footnote 8 only requires that the proposed standard include timelines for certain elements, without specificity for what those timeframes should be. The bright line CIP version 5 applicability that is used within this standard became effective 02-03-14 and was giving industry 24 months to implement. The CIP-014 draft appears to assume those bright line considerations are already completed for industry and provides just over 6 months to complete an additional assessment to remain compliant. Without specific implementation timeframes provided by FERC, and to stay in closer alignment to the expected completion dates for CIP v5, Tri-State is recommending no less than a one year after this standard becomes effective for the R1 risk assessment to be completed.
Hydro One	Yes	Will FERC accept R2.3 and R6.3, which allows the TO or TOP to document why they are not following the recommendations from the verification? The FERC Order did not suggest this.It is extremely important that all jurisdictions follow the same standard, so that the mitigation of risk to physical security is consistent. Having some jurisdictions who follow a more stringent standard will increase costs to ratepayers in those jurisdictions.The standard should provide a definition for "unaffiliated".

Organization	Yes or No	Question 4 Comment
Colorado Springs Utilities	Yes	
Empire District Electric Company	Yes	
OPG	Yes	
The Empire District Electric Company	Yes	
Herb Schrayshuen	Yes	The Implementation Plan can be read that it obligates applicable entities to complete the initial risk assessment in Requirement R1, on or before the effective date of the standard. The implementation plan should be adjusted. The following is a suggestion to facilitate reading of the standard and stay whitn defined terms without introfucing new terms which are undefined: For all requirements: Replace the expression "Transmission stations and Transmission substations" with "Transmission facilities". Otherwise, please explain why such a distinction is necessary. While the requirement for unaffiliated third party verification of the physical security plan is something required by the FERC in its order, the mandate is misguided and will lead to security breaches while at the same time adding no incremental value to the physical security plan. The utility, which owns the assets, is already highly incentivized to put together a good security plan to avoid loss of its facilities to terrorism without third party verification. The utility may decide to use security consultants to help develop the plan if it involves new, state of the art physical security topics outside the utilities experience base. On balance the third party verification requirement outlined in R6 regarding the physical security plan is unneeded.
NIPSCO		In R2 we are not sure who would do the verification. On one of the webinars a member of PJM suggested that another PJM member could be a candidate. However

Organization	Yes or No	Question 4 Comment
		it is likely that a PJM member is not a PC, TP or RC as prescribed in the requirement; that role is performed by PJM itself. Any further guidance would be welcome; we do not consider this a "show stopper".The hard work that went into putting this project together in such a short time frame is appreciated, thanks.

Additional comment received from Marcus Pelt, Southern Company

“The wording of Requirement R2.s, as it stands currently, could be interpreted to place requirements on the unaffiliated third party verifier when the responsible entity is actually the Transmission Owner. Southern recommends that R2.2 be reworded as follows to address this concern:

END OF REPORT

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the Standard Drafting Team (SDT) for Project 2014-04 Physical Security were solicited March 13-18, 2014, and the SDT was appointed by the Standards Committee on March 21, 2014.
2. Technical Conference was held April 1, 2014.
3. The draft standard was posted, pursuant to a Standards Committee authorized waiver, for a 15-day Formal Comment Period with a 5-day Initial Ballot April 10-24, 2014.

Description of Current Draft

This is the second draft of the proposed Reliability Standard, and it is being posted for final ballot. This draft includes proposed requirements to meet the directives issued in the FERC order issued March 7, 2014, in Docket No. RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Anticipated Actions	Anticipated Date
5-day Final Ballot, pursuant to a Standards Committee authorized waiver.	May 1, 2014
BOT Adoption.	May 2014
File with applicable Regulatory Authorities.	No later than June 5, 2014

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Effective Date	New

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

A. Introduction

1. Title: Physical Security

2. Number: CIP-014-1

3. Purpose: To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. Applicability:

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread

instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or

- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term “unaffiliated” means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term “unaffiliated” is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is a functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1, Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement

R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical

security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

R6. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally,

examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

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 during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three 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, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 Applicability

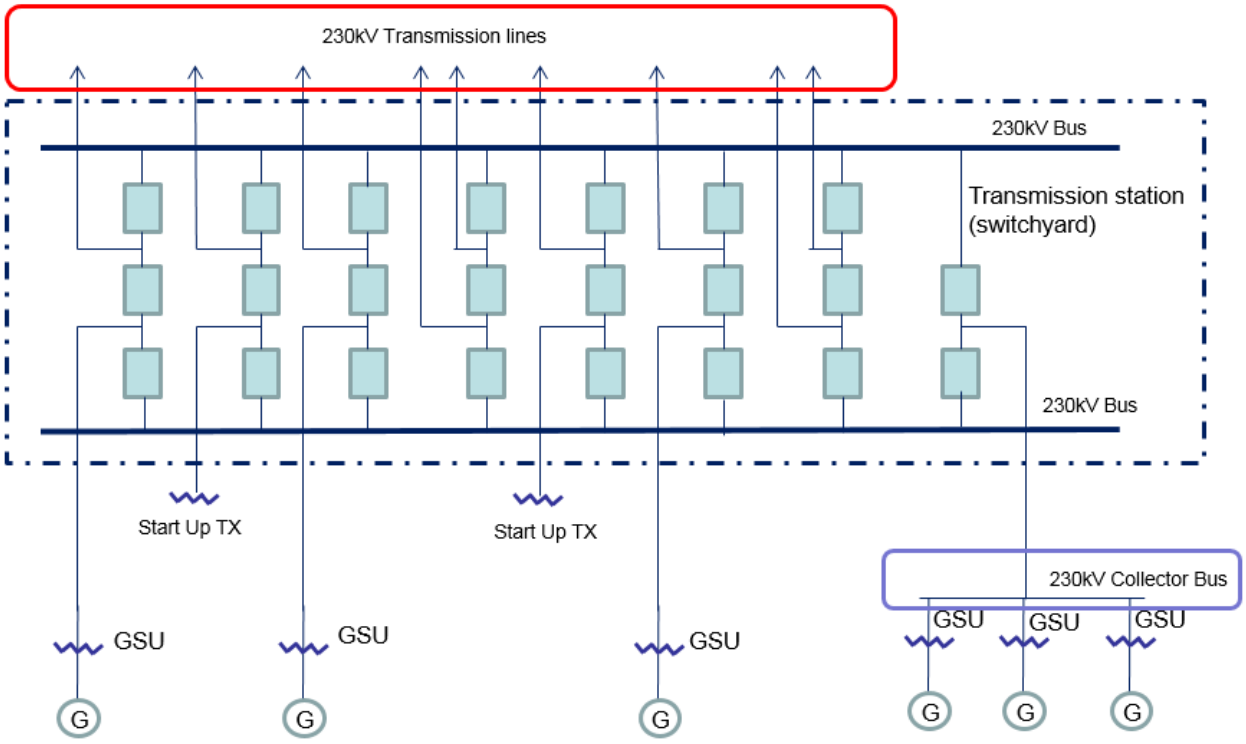
The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators. A Transmission Operator's obligations under the standard, however, are only triggered if the Transmission Operator is notified by an applicable Transmission Owner under Requirement R3 that the Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within

an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers that, if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014-1, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014-1 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014-1 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the

Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following guidance is only an example on how a Transmission Owner may perform a power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a significant area of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result in potential widespread instability, uncontrolled separation, or Cascading within an Interconnection. Regional consultation on these matters is likely to be helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes widespread instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.

2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.
3. Review of the Requirement R1 risk assessment methodology.

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.

- The entity's familiarity with the Interconnection within which the Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk

assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and Emergency Medical Services.

- *A timeline for executing the physical security enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

  Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the Transmission Owner or Transmission Operator with appropriate expertise for the evaluation performed according to

Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected third party reviewer cannot be a corporate affiliate (*i.e.,* the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

  In selecting CPP and PSP for use in this standard, the SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*

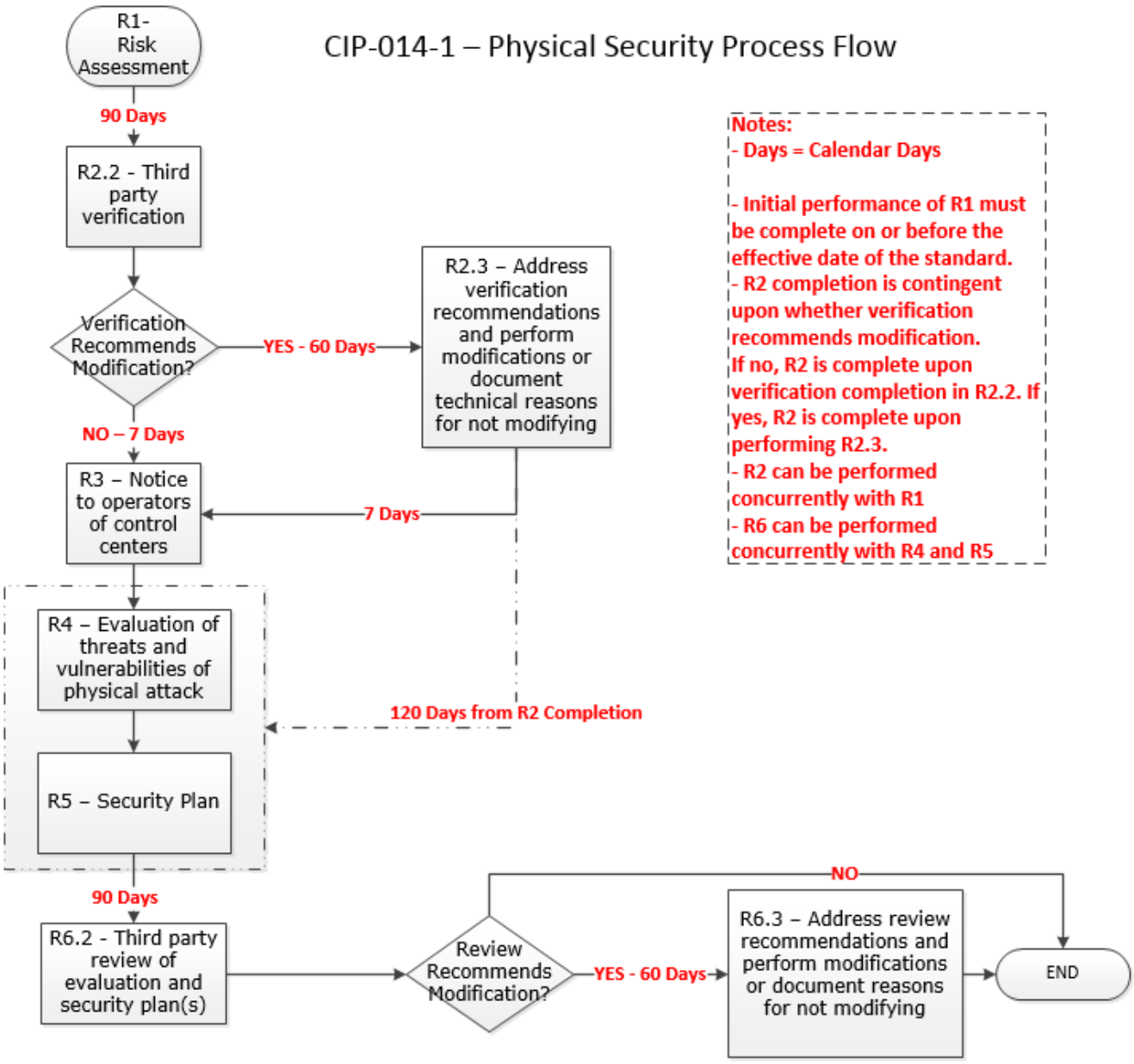
- *A governmental agency with physical security expertise.*

- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

As with the verification under Requirement R2, Requirement R6 provides that the "review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a Transmission Owner or Transmission Operator could collaborate with their unaffiliated third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) to satisfy Requirements R4 through R6 simultaneously. The

intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

Timeline


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
NO
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. Nominations for the Standard Drafting Team (SDT) for Project 2014-04 Physical Security were solicited March 13-18, 2014, and the SDT was appointed by the Standards Committee on March 21, 2014.
2. Technical Conference was held April 1, 2014.
3. The draft standard was posted, pursuant to a Standards Committee authorized waiver, for a 15-day Formal Comment Period with a 5-day Initial Ballot April 10-24, 2014.

Description of Current Draft

This is the ~~first~~second draft of the proposed Reliability Standard, and it is being posted for ~~stakeholder comment and initial~~final ballot. This draft includes proposed requirements to meet the directives issued in the FERC order issued March 7, 2014, in Docket No. RD14-6-000, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014).

Anticipated Actions	Anticipated Date
~~15-day Formal Comment Period with a 5-day Initial Ballot, pursuant to a Standards Committee authorized waiver.~~	~~April 10, 2014~~
~~10-day Formal Comment Period with a~~ 5-day ~~Additional~~Final Ballot ~~(if necessary),~~ pursuant to a Standards Committee authorized waiver.	May 1, 2014
~~5-day Final Ballot, pursuant to a Standards Committee authorized waiver.~~	~~May 2014~~
BOT Adoption.	May 2014
File with applicable Regulatory Authorities.	No later than June 5, 2014

Version History

Version	Date	Action	Change Tracking
1.0	TBD	Effective Date	New

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the NERC Glossary of Terms used in Reliability Standards (Glossary) are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

None

A. Introduction

1. **Title:** Physical Security

2. **Number:** CIP-014-1

3. **Purpose:** To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

4. **Applicability:**

4.1. Functional Entities:

4.1.1 Transmission Owner that owns a Transmission station or Transmission substation that meets any of the following criteria:

4.1.1.1 Transmission Facilities operated at 500 kV or higher. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

4.1.1.2 Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value" exceeding 3000 according to the table below. The "aggregate weighted value" for a single station or substation is determined by summing the "weight value per line" shown in the table below for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation. For the purpose of this criterion, the collector bus for a generation plant is not considered a Transmission Facility, but is part of the generation interconnection Facility.

Voltage Value of a Line	Weight Value per Line
less than 200 kV (not applicable)	(not applicable)
200 kV to 299 kV	700
300 kV to 499 kV	1300
500 kV and above	0

4.1.1.3 Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or

Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies.

4.1.1.4 Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

4.1.2 Transmission Operator.

Exemption: Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission ~~or~~are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

5. Effective Dates:

CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities, or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

6. Background:

This Reliability Standard addresses the directives from the FERC order issued March 7, 2014, *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014), which required NERC to develop a physical security reliability standard(s) to identify and protect facilities that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

B. Requirements and Measures

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify ~~any~~the Transmission station(s) and Transmission substation(s) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. *[VRF: High; Time-Horizon: Long-term Planning]*

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or

- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Rationale for Requirement R1:

This requirement meets the FERC directive from paragraph 6 in the order on physical security to perform a risk assessment to identify which facilities if rendered inoperable or damaged could impact an Interconnection through widespread

instability, uncontrolled separation, or cascading failures. It also meets the portion of the directive from paragraph 11 for periodic reevaluation by requiring the risk assessment to be performed every 30 months (or 60 months for an entity that has not identified in a previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection).

After identifying each Transmission station and Transmission substation that meets the criteria in Requirement R1, it is important to additionally identify the primary control center that operationally controls that Transmission station or Transmission substation (*i.e.,* the control center whose electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker, compared to a control center that only has the ability to monitor the Transmission station and Transmission substation and, therefore, must coordinate direct physical action through another entity).

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1. *[VRF: Medium; Time-Horizon: Long-term Planning]*

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated ~~verifying entity~~third party verification shall ~~either~~ verify the Transmission Owner's risk assessment performed under Requirement R1 ~~or recommend~~, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:

- Modify its identification under Requirement R1 consistent with the recommendation; or

- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~made available to the unaffiliated third party ~~verif~~verifier ~~ying entity~~ and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third party verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Rationale for Requirement R2:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring verification by an entity other than the owner or operator of the risk assessment performed under Requirement R1.

This requirement provides the flexibility for a Transmission Owner to select registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term "unaffiliated" means that the selected verifying entity cannot be a corporate affiliate (*i.e.*, the verifying entity cannot be an entity that controls, is controlled by, or is under common control with, the Transmission owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit. The term "unaffiliated" is not intended to prohibit a governmental entity from using another government entity to be a verifier under Requirement R2.

Requirement R2 also provides the Transmission Owner the flexibility to work with the verifying entity throughout the Requirement R1 risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could coordinate with their unaffiliated verifying entity to perform a Requirement R1 risk assessment to satisfy both Requirement R1 and Requirement R2 concurrently.

Planning Coordinator is functional entity listed in Part 2.1. The Planning Coordinator and Planning Authority are the same entity as shown in the NERC Glossary of Terms Used in NERC Reliability Standards.

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1 ~~and~~ , Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2 ~~that~~ , and b) is not under the operational control of the Transmission Owner~~,~~ : the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2. *[VRF: Lower; Time-Horizon: Long-term Planning]*

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Rationale for Requirement R3:

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first identifying which Transmission stations and Transmission substations meet the criteria specified by Requirement R1, as verified according to Requirement R2. This requirement is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 ~~and~~ , Part 1.2 of a Transmission station or Transmission substation verified according to Requirement R2 receives notice of such identification so that the Transmission Operator may timely fulfill its resulting obligations under Requirements R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include notice of the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or the verification process under Requirement R2.

R4. Each Transmission Owner that ~~owns or operates~~ identified a Transmission station, Transmission substation, or a primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall conduct an evaluation of the potential threats and

vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: *[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]*

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history ~~or~~of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Rationale for Requirement R4:

This requirement meets the FERC directive from paragraph 8 in the order on physical security that the reliability standard must require tailored evaluation of potential threats and vulnerabilities to facilities identified in Requirement R1 and verified according to Requirement R2. Threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections, and attractiveness of the target. As such, the requirement does not mandate a one-size-fits-all approach but requires entities to account for the unique characteristics of their facilities.

Requirement R4 does not explicitly state when the evaluation of threats and vulnerabilities must occur or be completed. However, Requirement R5 requires that the entity's security plan(s), which is dependent on the Requirement R4 evaluation, must be completed within 120 calendar days following completion of Requirement R2. Thus, an entity has the flexibility when to complete the Requirement R4 evaluation, provided that it is completed in time to comply with the requirement in Requirement R5 to develop a physical security plan 120 calendar days following completion of Requirement R2.

R5. Each Transmission Owner that ~~owns or has operational control of~~ identified a Transmission station, Transmission substation, or primary control center ~~identified~~ in

Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s~~)~~). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2~~.~~ and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: *[VRF: High; Time-Horizon: Long-term Planning]*

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for ~~implementing~~executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating ~~implementation~~ execution of the physical security plan according to the timeline specified in the physical security plan.

Rationale for Requirement R5:

This requirement meets the FERC directive from paragraph 9 in the order on physical security requiring the development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

R6. Each Transmission Owner that ~~owns or operates~~ identified a Transmission station, Transmission substation, or primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or~~

~~Transmission substation~~, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. *[VRF: Medium; Time-Horizon: Long-term Planning]*

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

~~**6.1.1.**~~ An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.

~~**6.1.2.**~~ An entity or organization approved by the ERO.

~~**6.1.3.**~~ A governmental agency with physical security expertise.

~~**6.1.4.**~~ An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated ~~reviewing entity~~third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with~~made available to the unaffiliated third party reviewer~~ing entity and from any other form of public disclosure~~ and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

Rationale for Requirement R6:

This requirement meets the FERC directive from paragraph 11 in the order on physical security requiring review by an entity other than the owner or operator with appropriate expertise of the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5.

As with the verification required by Requirement R2, Requirement R6 provides Transmission Owners and Transmission Operators the flexibility to work with the third party reviewer~~ing entity~~ throughout the Requirement R4 evaluation and the development of the Requirement R5 security plan(s). This would allow entities to satisfy their obligations under Requirement R6 concurrent with the satisfaction of their obligations under Requirements R4 and R5.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

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

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 during an on-site visit to show that it was compliant for the full time period since the last audit.

The Transmission Owner and Transmission Operator shall keep data or evidence to show compliance, as identified below, unless directed by its Compliance Enforcement Authority (CEA) to retain specific evidence for a longer period of time as part of an investigation.

The responsible entities shall retain documentation as evidence for three 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, subject to the confidentiality provisions of Section 1500 of the Rules of Procedure and the provisions of Section 1.4 below.

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints Text

1.4. Additional Compliance Information

Confidentiality: To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities.

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Long-term Planning**	**High**	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an	instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection	Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability,

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.	Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.	performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.	uncontrolled separation, or Cascading within an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months;

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
R2	**Long-term Planning**	**Medium**	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to	The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			less than or equal to 100 calendar days following completion of Requirement R1; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by ~~part~~Part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.	less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by ~~part~~Part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.	120 calendar days following completion of Requirement R1; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by ~~part~~Part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed	following completion of Requirement R1; OR The Transmission Owner failed to have ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1; OR The Transmission Owner had ~~a~~an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by ~~part~~Part 2.3.	
R3	**Long-term Planning**	**Lower**	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.	operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.	of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.	center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						identification in Requirement R1.
R4	**Operations Planning, Long-term Planning**	**Medium**	N/A	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
R5	**Long-term Planning**	**High**	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.	The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.	The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						center(s) identified in Requirement R1 and verified according to Requirement 2 but failed to include Parts 5.1 through 5.4 in the plan.
R6	**Long-term Planning**	**Medium**	The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement	The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed	The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed	The Responsible Entity failed to have ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and

R #	Time Horizon	VRF	Violation Severity Levels (CIP-014-1)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.	under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.	under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not ~~and modify or~~ document the reason for not modifying the security plan(s) as specified in Part 6.3.	the security plan(s) developed under Requirement R5; OR The Responsible Entity had ~~a~~an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Guidelines and Technical Basis

Section 4 Applicability

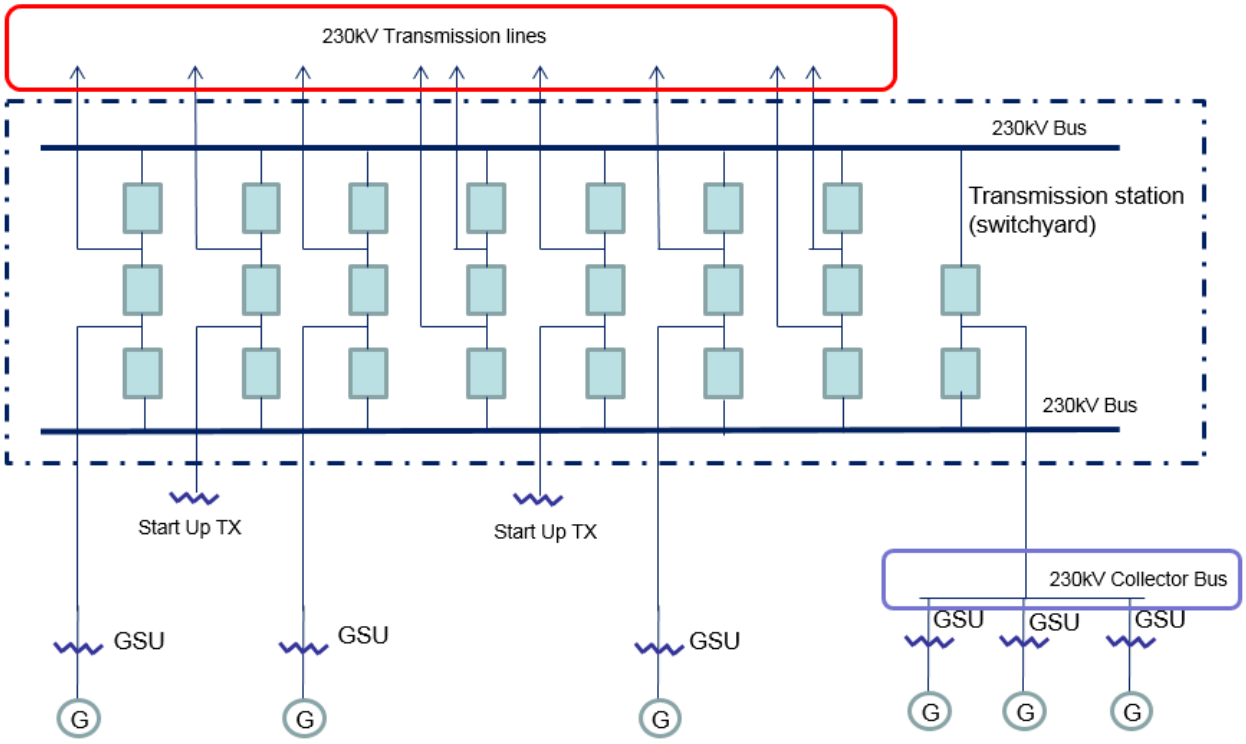
The purpose of Reliability Standard CIP-014-1 is to protect Transmission stations and Transmission substations, and their associated primary control centers~~,~~ that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. To properly include those entities that own or operate such Facilities, the Reliability Standard CIP-014-1 first applies to Transmission Owners ~~(TO)~~ that own Transmission Facilities that meet the specific criteria in Applicability Section 4.1.1.1 through 4.1.1.4. The Facilities described in Applicability Section 4.1.1.1 through 4.1.1.4 mirror those Transmission Facilities that meet the bright line criteria for "Medium Impact" Transmission Facilities under Attachment 1 of Reliability Standard CIP-002-5.1. Each ~~TO~~Transmission Owner that owns Transmission Facilities that meet the criteria in Section 4.1.1.1 through 4.1.1.4 is required to perform a risk assessment as specified in Requirement R1 to identify its Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Standard Drafting Team (SDT) expects this population will be small and that many ~~TOs~~Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities. Only those ~~TOs~~Transmission Owners with Transmission stations or Transmission substations identified in the risk assessment (and verified under Requirement R2) have performance obligations under Requirements R3 through R6.

This standard also applies to Transmission Operators ~~(TOP).~~ A ~~TOP's~~Transmission Operator's obligations under the standard, however, are only triggered if the ~~TOP~~Transmission Operator is notified by an applicable ~~TO~~Transmission Owner under Requirement R3 that the ~~TOP~~Transmission Operator operates a primary control center that operationally controls a Transmission station(s) or Transmission substation(s) identified in the Requirement R1 risk assessment. A primary control center operationally controls a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker, as opposed to a control center that only has information from the Transmission station or Transmission substation and must coordinate direct action through another entity. Only ~~TOPs~~Transmission Operators who are notified that they have primary control centers under this standard have performance obligations under Requirements R4 through R6. In other words, primary control center for purposes of this Standard is the control center that the Transmission Owner or Transmission Operator, respectively, uses as its primary, permanently-manned site to physically operate a Transmission station or Transmission substation that is identified in Requirement R1 and verified in Requirement R2. Control centers that provide back-up capability are not applicable, as they are a form of resiliency and intentionally redundant.

The ~~drafting team~~SDT considered several options for bright line criteria that could be used to determine applicability and provide an initial threshold that defines the set of Transmission stations and Transmission substations that would meet the directives of the FERC order on

physical security (*i.e.*, those that could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection). The SDT determined that using the criteria for Medium Impact Transmission Facilities in Attachment 1 of CIP-002-5.1 would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. Additionally, the SDT concluded that using the CIP-002-5.1 Medium Impact criteria was appropriate because it has been approved by stakeholders, NERC, and FERC, and its use provides a technically sound basis to determine which Transmission Owners should conduct the risk assessment. As described in CIP-~~005-2~~002-5.1, the failure of a Transmission station or Transmission substation that meets the Medium Impact criteria could have the capability to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs). The SDT understands that using this bright line criteria to determine applicability may require some Transmission Owners to perform risk assessments under Requirement R1 that will result in a finding that none of their Transmission stations or Transmission substations would pose a risk of widespread instability, uncontrolled separation, or Cascading within an Interconnection. However, the SDT determined that higher bright lines could not be technically justified to ensure inclusion of all Transmission stations and Transmission substations, and their associated primary control centers~~,~~ that, if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. Further guidance and technical basis for the bright line criteria for Medium Impact Facilities can be found in the Guidelines and Technical Basis section of CIP-002-5.1.

Additionally, the SDT determined that it was not necessary to include Generator Operators and Generator Owners in the Reliability Standard. ~~First, the transmission analysis or analyses conducted under Requirement R1 will~~First, Transmission stations or Transmission substations interconnecting generation facilities are considered when determining applicability. Transmission Owners will consider those Transmission stations and Transmission substations that include a Transmission station on the high side of the Generator Step-up transformer (GSU) using Applicability Section Parts 4.1.1.1 and 4.1.1.2. As an example, a Transmission station or Transmission substation identified as a Transmission Owner facility that interconnects generation will be subject to the Requirement R1 risk assessment if it operates at 500kV or greater or if it is connected at 200 kV – 499kV to three or more other Transmission stations or Transmission substations and has an "aggregate weighted value" exceeding 3000 according to the table in Applicability Section Part 4.1.1.2. Second, the Transmission analysis or analyses conducted under Requirement R1 should take into account the impact of the loss of generation connected to applicable Transmission stations or Transmission substations~~..~~. Additionally, the FERC order does not explicitly mention generation assets and is reasonably understood to focus on the most critical Transmission Facilities. The diagram below shows an example of a station.



Also, the SDT uses the phrase "Transmission stations or Transmission substations" to recognize the existence of both stations and substations. Many entities in industry consider a substation to be a location with physical borders (i.e. fence, wall, etc.) that contains at least an autotransformer. Locations also exist that do not contain autotransformers, and many entities in industry refer to those locations as stations (switching stations or switchyards). Therefore, the SDT chose to use both "station" and "substation" to refer to the locations where groups of Transmission Facilities exist.

On the issue of joint ownership, the SDT recognizes that this issue is not unique to CIP-014-1, and expects that the applicable Transmission Owners and Transmission Operators will develop memorandums of understanding, agreements, Coordinated Functional Registrations, or procedures, etc., to designate responsibilities under CIP-014-1 when joint ownership is at issue, which is similar to what many entities have completed for other Reliability Standards.

The language contained in the applicability section regarding the collector bus is directly copied from CIP-002-5.1, Attachment 1, and has no additional meaning within the CIP-014-1 standard.

Requirement R1

The initial risk assessment required under Requirement R1 must be completed on or before the effective date of the standard. Subsequent risk assessments are to be performed at least once

every 30 or 60 months depending on the results of the previous risk assessment per Requirement R1, Part 1.1. In performing the risk assessment under Requirement R1, the Transmission Owner should first identify their population of Transmission stations and Transmission substations that meet the criteria contained in Applicability Section 4.1.1. Requirement R1 then requires the Transmission Owner to perform a risk assessment, consisting of a transmission analysis, to determine which of those Transmission stations and Transmission Substations if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The standard does not mandate the specific analytical method for performing the risk assessment. The Transmission Owner has the discretion to choose the specific method that best suites its needs. As an example, an entity may perform a Power Flow analysis and stability analysis at a variety of load levels.

Performing Risk Assessments

The Transmission Owner has the discretion to select a transmission analysis method that fits its facts and system circumstances. To mandate a specific approach is not technically desirable and may lead to results that fail to adequately consider regional, topological, and system circumstances. The following ~~is~~ guidance is only an example on how a Transmission Owner may perform a ~~traditional~~ power flow and/or stability analysis to identify those Transmission stations and Transmission substations that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. An entity could remove all lines, without regard to the voltage level, to a single Transmission station or Transmission substation and review the simulation results to assess system behavior to determine if Cascading of Transmission Facilities, uncontrolled separation, or voltage or frequency instability is likely to occur over a ~~wide~~significant area~~.~~ of the Interconnection. Using engineering judgment, the Transmission Owner (possibly in consultation with regional planning or operation committees and/or ISO/RTO committee input) should develop criteria (e.g. imposing a fault near the removed Transmission station or Transmission substation) to identify a contingency or parameters that result~~ing~~ in potential widespread instability, uncontrolled separation, or Cascading within an Interconnection. ~~For example, the criteria~~Regional consultation on these matters is likely to be helpful and informative, given that the inputs for the risk assessment and the attributes of what constitutes widespread instability, uncontrolled separation, or Cascading within an Interconnection will likely vary from region-to-region or from ISO-to-ISO based on topology, system characteristics, and system configurations. Criteria could also include post-contingency facilities loadings above a certain emergency rating or failure of a power flow case to converge. Available ~~remedial action schemes (RAS) or~~ special protection systems (SPS), if any, could be applied to determine if the system experiences any additional instability which may result in uncontrolled separation. Example criteria may include:

(a) Thermal overloads beyond facility emergency ratings;

(b) Voltage deviation exceeding ± 10%; or

(c) Cascading outage/voltage collapse; or

(d) Frequency below under-frequency load shed points

Periodicity

~~A TO~~A Transmission Owner who identifies one or more Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection is required to conduct a risk assessment at least once every 30 months. This period ensures that the risk assessment remains current with projected conditions and configurations in the planned system. This risk assessment, as the initial assessment, must consider applicable planned Transmission stations and Transmission substations to be in service within 24 months. The 30 month timeframe aligns with the 24 month planned to be in service date because the Transmission Owner is provided the flexibility, depending on its planning cycle and the frequency in which it may plan to construct a new Transmission station or Transmission substation to more closely align these dates. The requirement is to conduct the risk assessment at least once every 30 months, so for a Transmission Owner that believes it is better to conduct a risk assessment once every 24 months, because of its planning cycle, it has the flexibility to do so.

~~TOs who~~Transmission Owners that have not identified any Transmission stations or Transmission substations (as verified under Requirement R2) that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection are unlikely to see changes to their risk assessment in the Near-Term Planning Horizon. Consequently, a 60 month periodicity for completing a subsequent risk assessment is specified.

Identification of Primary Control Centers

After completing the risk assessment specified in Requirement R1, it is important to additionally identify the primary control center that operationally controls each Transmission station or Transmission substation that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. A primary control center "operationally controls" a Transmission station or Transmission substation when the control center's electronic actions can cause direct physical actions at the identified Transmission station and Transmission substation, such as opening a breaker.

Requirement R2

This requirement specifies verification of the risk assessment performed under Requirement R1 by an entity other than the owner or operator of the Requirement R1 risk assessment.

A verification of the risk assessment by an unaffiliated third party, as specified in Requirement R2, could consist of:

1. Certifying that the Requirement R1 risk assessment considers the Transmission stations and Transmission substations identified in Applicability Section 4.1.1.
2. Review of the model used to conduct the risk assessment to ensure it contains sufficient system topology to identify Transmission stations and Transmission substations that if

rendered inoperable or damaged could cause widespread instability, uncontrolled separation, or Cascading within an Interconnection.

3. Review of the Requirement R1 risk assessment ~~method, which may include, for example, consideration of factors such as the following system performance criteria:~~methodology.

   ~~a. Thermal overloads beyond facility emergency ratings;~~

   ~~b. Voltage deviation exceeding ± 10%,~~

   ~~c. Cascading outage/Voltage collapse,~~

   ~~Frequency below under-frequency load shed points.~~

This requirement provides the flexibility for a Transmission Owner to select from unaffiliated registered and non-registered entities with transmission planning or analysis experience to perform the verification of the Requirement R1 risk assessment. The term unaffiliated means that the selected verifying entity cannot be a corporate affiliate (*i.e.,* the verifying or ~~reviewing entity~~third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Owner). The verifying entity also cannot be a division of the Transmission Owner that operates as a functional unit.

The prohibition on registered entities using a corporate affiliate to conduct the verification, however, does not prohibit a governmental entity (e.g., a city, a municipality, a U.S. federal power marketing agency, or any other political subdivision of U.S. or Canadian federal, state, or provincial governments) from selecting as the verifying entity another governmental entity within the same political subdivision. For instance, a U.S. federal power marketing agency may select as its verifier another U.S. federal agency to conduct its verification so long as the selected entity has transmission planning or analysis experience. Similarly, a Transmission Owner owned by a Canadian province can use a separate agency of that province to perform the verification. The verifying entity, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

Requirement R2 also provides that the "verification may occur concurrent with or after the risk assessment performed under Requirement R1." This provision is designed to provide the Transmission Owner the flexibility to work with the verifying entity throughout (*i.e.,* concurrent with) the risk assessment, which for some Transmission Owners may be more efficient and effective. In other words, a Transmission Owner could ~~coordinate~~collaborate with their unaffiliated verifying entity to perform the risk assessment under Requirement R1 such that both Requirement R1 and Requirement R2 are satisfied concurrently. The intent of Requirement R2 is to have an entity other than the owner or operator of the facility to be involved in the risk assessment process and have an opportunity to provide input. Accordingly, Requirement R2 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the risk assessment and subsequently has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the risk assessment.

Characteristics to consider in selecting a ~~reviewing entity~~third party reviewer could include:

- Registered Entity with applicable planning and reliability functions.
- Experience in power system studies and planning.
- The entity's understanding of the MOD standards, TPL standards, and facility ratings as they pertain to planning studies.
- The entity's familiarity with the Interconnection within which the ~~transmission owner~~Transmission Owner is located.

With respect to the requirement that Transmission owners develop and implement procedures for protecting confidential and sensitive information, the Transmission Owner could have a method for identifying documents that require confidential treatment. One mechanism for protecting confidential or sensitive information is to prohibit removal of sensitive or confidential information from the ~~TO's~~Transmission Owner's site. Transmission Owners could include such a prohibition in a non-disclosure agreement with the verifying entity.

A Technical feasibility study is not required in the Requirement R2 documentation of the technical basis for not modifying the identification in accordance with the recommendation.

On the issue of the difference between a verifier in Requirement R2 and a reviewer in Requirement R6, the SDT indicates that the verifier will confirm that the risk assessment was completed in accordance with Requirement R1, including the number of Transmission stations and substations identified, while the reviewer in Requirement R6 is providing expertise on the manner in which the evaluation of threats was conducted in accordance with Requirement R4, and the physical security plan in accordance with Requirement R5. In the latter situation there is no verification of a technical analysis, rather an application of experience and expertise to provide guidance or recommendations, if needed.

Parts 2.4 and 6.4 require the entities to have procedures to protect the confidentiality of sensitive or confidential information. Those procedures may include the following elements:

1. Control and retention of information on site for third party verifiers/reviewers.
2. Only "need to know" employees, etc., get the information.
3. Marking documents as confidential
4. Securely storing and destroying information when no longer needed.
5. Not releasing information outside the entity without, for example, General Counsel sign-off.

Requirement R3

Some Transmission Operators will have obligations under this standard for certain primary control centers. Those obligations, however, are contingent upon a Transmission Owner first completing the risk assessment specified by Requirement R1 and the verification specified by Requirement R2. Requirement R3 is intended to ensure that a Transmission Operator that has operational control of a primary control center identified in Requirement R1 receive notice so that the Transmission Operator may fulfill the rest of the obligations required in Requirements

R4 through R6. Since the timing obligations in Requirements R4 through R6 are based upon completion of Requirement R2, the Transmission Owner must also include within the notice the date of completion of Requirement R2. Similarly, the Transmission Owner must notify the Transmission Operator of any removals from identification that result from a subsequent risk assessment under Requirement R1 or as a result of the verification process under Requirement R2.

Requirement R4

This requirement requires owners and operators of facilities identified by the Requirement R1 risk assessment and that are verified under Requirement R2 to conduct an assessment of potential threats and vulnerabilities to those Transmission stations, Transmission substations, and primary control centers using a tailored evaluation process. Threats and vulnerabilities may vary from facility to facility based on any number of factors that include, but are not limited to, location, size, function, existing physical security protections, and attractiveness as a target.

In order to effectively conduct a threat and vulnerability assessment, the asset owner may be the best source to determine specific site vulnerabilities, but current and evolving threats may best be determined by others in the intelligence or law enforcement communities. A number of resources have been identified in the standard, but many others exist and asset owners are not limited to where they may turn for assistance. Additional resources may include state or local fusion centers, U.S. Department of Homeland Security, Federal Bureau of Investigations (FBI), Public Safety Canada, Royal Canadian Mounted Police, and InfraGard chapters coordinated by the FBI.

The Responsible Entity is required to take a number of factors into account in Parts 4.1 to 4.3 in order to make a risk-based evaluation under Requirement R4.

To assist in determining the current threat for a facility, the prior history of attacks on similarly protected facilities should be considered when assessing probability and likelihood of occurrence at the facility in question.

Resources that may be useful in conducting threat and vulnerability assessments include:

- NERC Security Guideline for the Electricity Sector: Physical Security.
- NERC Security Guideline: Physical Security Response.
- ASIS International General Risk Assessment Guidelines.
- ASIS International Facilities Physical Security Measure Guideline.
- ASIS International Security Management Standard: Physical Asset Protection.
- Whole Building Design Guide - Threat/Vulnerability Assessments.

Requirement R5

This requirement specifies development and implementation of a security plan(s) designed to protect against attacks to the facilities identified in Requirement R1 based on the assessment performed under Requirement R4.

Requirement R5 specifies the following attributes for the physical security plan:

- *Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on~~identified during the ~~results of the assessment~~evaluation conducted in Requirement R4.~~.~~.*

  Resiliency may include, among other things:

  a. System topology changes,

  b. Spare equipment,

  c. Construction of a new Transmission station or Transmission substation.

  While most security measures will work together to collectively harden the entire site, some may be allocated to protect specific critical components. For example, if protection from gunfire is considered necessary, the entity may only install ballistic protection for critical components, not the entire site.

- *Law enforcement contact and coordination information.*

  Examples of such information may be posting 9-1-1 for emergency calls and providing substation safety and familiarization training for local and federal law enforcement, fire department, and ~~EMS~~Emergency Medical Services.

- *A timeline for ~~implementing~~executing the physical security ~~resiliency or security measures~~enhancements and modifications specified in the physical security plan.*

  Entities have the flexibility to prioritize the implementation of the various resiliency or security ~~measures~~enhancements and modifications in their security plan according to risk, resources, or other factors. The requirement to include a timeline in the physical security plan for executing the actual physical security enhancements and modifications does not also require that the enhancements and modifications be completed within 120 days. The actual timeline may extend beyond the 120 days, depending on the amount of work to be completed.

- *Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).*

  A registered entity's physical security plan should include processes and responsibilities for obtaining and handling alerts, intelligence, and threat warnings from various sources. Some of these sources could include the ERO, ES-ISAC, and US and/or Canadian federal agencies. This information should be used to reevaluate or consider changes in the security plan and corresponding security measures of the security plan found in R5.

Incremental changes made to the physical security plan prior to the next required third party review do not require additional third party reviews.

Requirement R6

This requirement specifies review by an entity other than the ~~TO~~Transmission Owner or ~~TOP~~Transmission Operator with appropriate expertise for the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5. As with Requirement R2, the term unaffiliated means that the selected ~~reviewing entity~~third party reviewer cannot be a corporate affiliate (*i.e.,* the ~~reviewing entity~~third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Transmission Operator). A ~~reviewing entity~~third party reviewer also cannot be a division of the Transmission Operator that operates as a functional unit.

As noted in the guidance for Requirement R2, the prohibition on registered entities using a corporate affiliate to conduct the review, however, does not prohibit a governmental entity from selecting as the third party reviewer another governmental entity within the same political subdivision. For instance, a city or municipality may use its local enforcement agency, so long as the local law enforcement agency satisfies the criteria in Requirement R6. The third party reviewer, however, must still be a third party and cannot be a division of the registered entity that operates as a functional unit.

The Responsible Entity can select from several possible entities to perform the review:

- *An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.*

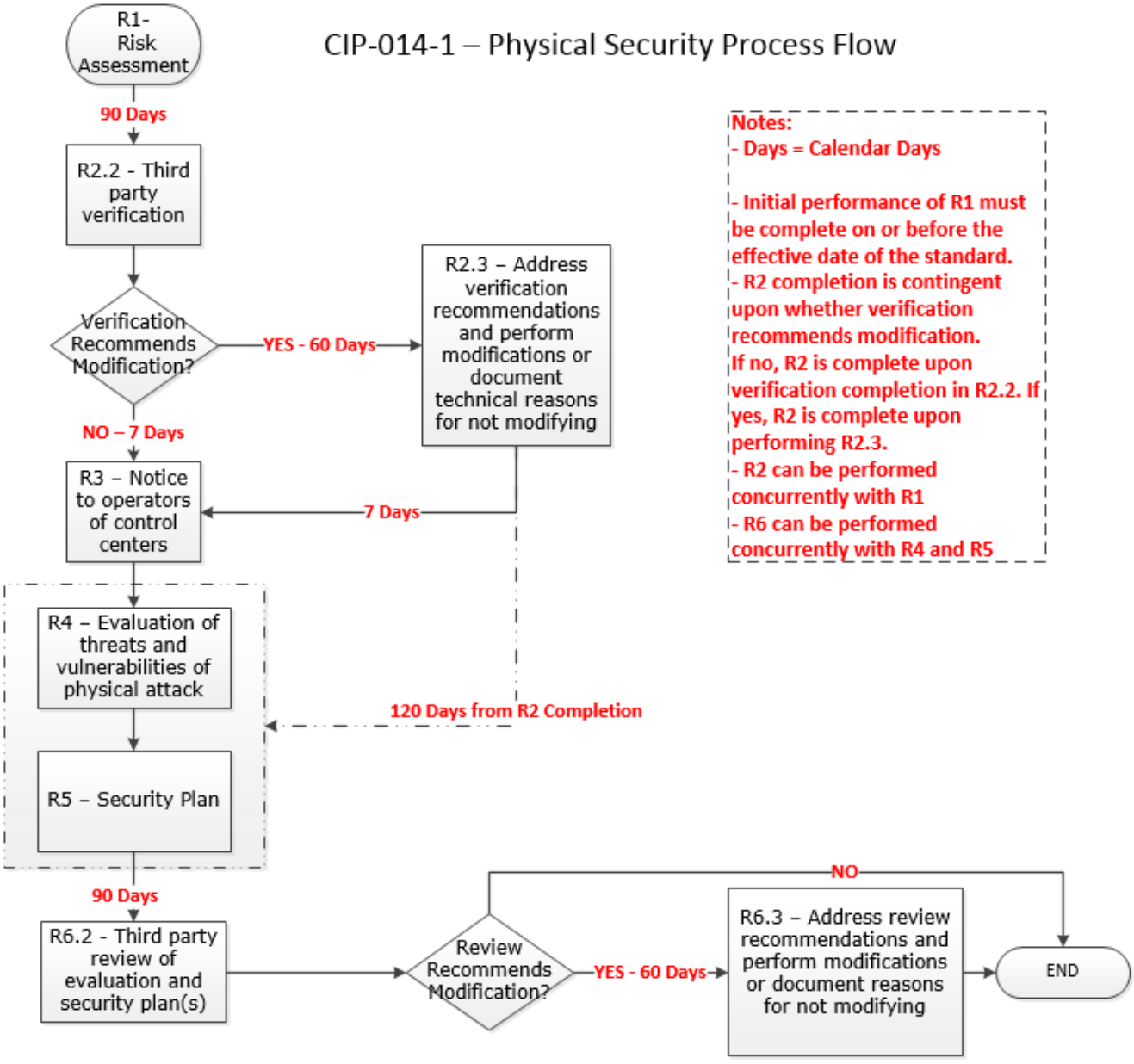
  In selecting CPP and PSP for use in this standard, the ~~drafting team~~SDT believed it was important that if a private entity such as a consulting or security firm was engaged to conduct the third party review, they must tangibly demonstrate competence to conduct the review. This includes electric industry physical security experience and either of the premier security industry certifications sponsored by ASIS International. The ASIS certification program was initiated in 1977, and those that hold the CPP certification are board certified in security management. Those that hold the PSP certification are board certified in physical security.

- *An entity or organization approved by the ERO.*
- *A governmental agency with physical security expertise.*
- *An entity or organization with demonstrated law enforcement, government, or military physical security expertise.*

~~A third party that contributes to the threat assessment and development of the security plan may also serve as the reviewer. As with Requirement R2, the Responsible Entity has~~As with the verification under Requirement R2, Requirement R6 provides that the "review may occur

concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5." This provision is designed to provide applicable Transmission Owners and Transmission Operators the flexibility to work with the ~~reviewing entity~~third party reviewer throughout (*i.e.,* concurrent with) the evaluation performed according to Requirement R4 and the security plan(s) developed according to Requirement R5, which for some Responsible Entities may be more efficient and effective. In other words, a ~~TO~~Transmission Owner or ~~TOP~~Transmission Operator could ~~coordinate~~collaborate with their unaffiliated ~~reviewing entity~~third party reviewer to perform an evaluation of potential threats and vulnerabilities (Requirement R4) and develop a security plan (Requirement R5) ~~concurrently with review to satisfy Requirements R4 through R6 simultaneously.~~to satisfy Requirements R4 through R6 simultaneously. The intent of Requirement R6 is to have an entity other than the owner or operator of the facility to be involved in the Requirement R4 evaluation and the development of the Requirement R5 security plans and have an opportunity to provide input on the evaluation and the security plan. Accordingly, Requirement R6 is designed to allow entities the discretion to have a two-step process, where the Transmission Owner performs the evaluation and develops the security plan itself and then has a third party review that assessment, or a one-step process, where the entity collaborates with a third party to perform the evaluation and develop the security plan.

~~Timeline~~


CIP-014-1 – Physical Security Process Flow
R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
NO
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
END
Notes:
- Days = Calendar Days
- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification. If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan for Project 2014-04

May 1, 2014

Approvals Requested
CIP-014-1 Physical Security

Prerequisite Approvals
None

Effective Date

New or Revised Standards
CIP-014-1 is effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. In those jurisdictions where regulatory approval is not required, CIP-014-1 shall become effective on the first day of the first calendar quarter that is six months beyond the date this standard is approved by the NERC Board of Trustees, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Standards for Retirement
None

Initial Performance of Periodic Requirements
The initial risk assessment required by CIP-014-1, Requirement R1, must be completed on or before the effective date of the standard. Subsequent risk assessments shall be performed according to the timelines specified in CIP-014-1, Requirement R1.

The initial performance of CIP-014-1, Requirements R2 through R6, must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows:

- Requirement R2 shall be completed as follows:
    - Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard.
    - Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2.

- Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.
- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2.
- Requirement R6 shall be completed as follows:
    - Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5.
    - Part 6.3 shall be completed within 60 calendar days of Requirement R6 part 6.2.

Consideration of Issues and Directives

Project 2014-04 - Physical Security

May 1, 2014

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
P.6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring Transmission Owners to perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line would provide a conservative threshold for defining which Transmission stations and Transmission substations must be included in the risk assessment in Requirement R1 of CIP-014-1. If the Transmission Owner does not have any Transmission stations or Transmission substations that meet the Medium

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		Impact rating, it is not subject to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the risk assessment is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed,	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
operated, and maintained, and the sophistication of recovery plans and inventory management.		
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the potential physical threats and vulnerabilities they face at the identified critical facilities.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring the applicable Transmission Owner or Transmission Operator of facilities identified in accordance with Requirement R1 and verified in accordance with Requirement R2 to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1) resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4; (2) law enforcement

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		contact and coordination information; (3) a timeline for executing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information that is needed to ensure compliance with the Reliability Standards.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to third party verifiers and reviewers and to protect or exempt sensitive or confidential information developed pursuant to the standard from public disclosure.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a	*Reliability Standards for Physical Security*	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated third party verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the verification shall either verify the Transmission Owner's risk assessment or include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The reviewing entity must be (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file the plan with the Reliability Standards for Commission review.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3 shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2.

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		- Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 Part 6.2.

Consideration of Issues and Directives

Project 2014-04 - Physical Security

~~April 9~~May 1, 2014

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
P.6. The Reliability Standards should require owners or operators of the Bulk-Power System to take at least three steps to address the risks that physical security attacks pose to the reliable operation of the Bulk-Power System. First, the Reliability Standards should require owners or operators of the Bulk-Power System to perform a risk assessment of their systems to identify their "critical facilities." A critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. Methodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment. The Commission is not requiring NERC to adopt a specific type of risk assessment, nor is the Commission requiring that a mandatory number of facilities be identified as critical facilities under the Reliability Standards. Instead, the Commission is directing NERC to develop Reliability	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R1 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring ~~that each~~ Transmission ~~Owner~~Owners to perform a risk assessment of its Transmission stations and substations that meet the criteria in Attachment 1 of CIP-002-5.1 for a Medium Impact rating to identify which of those Transmission stations and substations, if rendered inoperable or damaged as a result of a physical attack, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection. The Transmission Owner must also identify the primary control centers that operationally controls each identified Transmission station or Transmission substation. The standard drafting team (SDT) determined that the CIP-002-5 bright line ~~was appropriate because it has been vetted with stakeholders, and approved by NERC and FERC. The SDT concluded it was~~would provide a ~~technically sound basis to determine~~conservative threshold for defining which

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
Standards that will ensure that owners or operators of the Bulk-Power System identify those facilities that are critical to the reliable operation of the Bulk-Power System such that if those facilities are rendered inoperable or damaged, instability, uncontrolled separation or cascading failures could result on the Bulk-Power System and thereby warrant the directive imposed here.		Transmission ~~Owners should conduct~~stations and Transmission substations must be included in the risk assessment~~.~~ in Requirement R1 of CIP-014-1. If the Transmission Owner does not have any Transmission stations or Transmission substations that meet the Medium Impact rating, it is not subject to the proposed Reliability Standard and, in turn, would not have to conduct the risk assessment. Consistent with the Commission's directive, Requirement R1 does not require a specific methodology for identifying facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; rather, the requirement mandates that the risk assessment shall consist of a transmission analysis or transmission analyses to ensure that the ~~methodology~~risk assessment is based on objective analysis, technical expertise, and experienced judgment. Lastly, Requirement R1 identifies the periodicity for conducting the risk assessments.
7. Issuance of this directive will help provide for the resiliency and reliable operation of the Bulk-Power System. To that end, the proposed Reliability Standards should allow owners or operators to consider resilience of the grid in the risk assessment when identifying critical facilities, and the	*Reliability Standards for Physical Security Measures*, 146	Requirement R1 provides Transmission Owners the flexibility to consider the resilience of their system when conducting their risk assessments. As noted above, Requirement R1 does not require a specific methodology for identifying their critical facilities and, in turn, allows an entity to use a methodology that

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
elements that make up those facilities, such as transformers that typically require significant time to repair or replace. As part of this process, owners or operators may consider elements of resiliency such as how the system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.	FERC ¶ 61,166 (Mar. 7, 2014).	considers how their system is designed, operated, and maintained, and the sophistication of recovery plans and inventory management.
8. In the second step, the Reliability Standards should require owners or operators of the identified critical facilities to evaluate the potential threats and vulnerabilities to those identified facilities. The threats and vulnerabilities may vary from facility to facility based on factors such as the facility's location, size, function, existing protections and attractiveness as a target. Thus, the Reliability Standards should require the owners or operators to tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated. NERC should also consider in the standards development process requiring owners and operators to consult with entities with appropriate expertise as part of this evaluation process.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R4 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring that ~~each~~the applicable Transmission Owner ~~and~~or Transmission Operator ~~that owns or operates~~of facilities identified in accordance with Requirement R1 ~~(~~and verified ~~under~~in accordance with Requirement R2~~)~~ conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive to "tailor their evaluation to the unique characteristics of the identified critical facilities and the type of attacks that can be realistically contemplated," Requirement R4 states that the evaluation must consider: (1) the unique characteristics of the identified facilities; (2) prior history ~~or~~of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U. S. federal and/or Canadian governmental agencies, or their successors. Consistent with the Commission's statement that NERC should consider requiring owners and operators of identified facilities to consult with entities with appropriate expertise, Requirement R6 requires applicable Transmission Owners and Transmission Operators to select a third party to review their evaluation. This review may occur concurrently with or after the evaluation.
9. Third and finally, the Reliability Standards should require those owners or operators of critical facilities to develop and implement a security plan designed to protect against attacks to those identified critical facilities based on the assessment of the potential threats and vulnerabilities to their physical security. The Reliability Standards themselves need not dictate specific steps an entity must take to protect against attacks on the identified facilities. However, the Reliability Standards need to require that owners or operators of identified critical facilities have a plan that results in an adequate level of protection against the	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirement R5 of proposed Reliability Standard CIP-014-1 responds to this directive by requiring ~~that each~~the applicable Transmission Owner ~~and~~or Transmission Operator ~~that owns or operates~~of facilities identified in accordance with Requirement R1 ~~(~~and verified ~~under~~in accordance with Requirement R2~~)~~ to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). Consistent with the Commission's directive, Requirement R5 does not dictate specific steps an entity must take to protect against attacks on the identified facilities but requires applicable entities to develop a security plan that includes the following attributes to help ensure an adequate level of protection: (1)

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
potential physical threats and vulnerabilities they face at the identified critical facilities.		resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4; (2) law enforcement contact and coordination information; (3) a timeline for ~~implementing~~executing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
10. All three steps of compliance with the Reliability Standard described above could contain sensitive or confidential information that, if released to the public, could jeopardize the reliable operation of the Bulk-Power System. Guarding sensitive or confidential information is essential to protecting the public by discouraging attacks on critical infrastructure. Therefore, NERC should include in the Reliability Standards a procedure that will ensure confidential treatment of sensitive or confidential information but still allow for the Commission, NERC and the Regional Entities to review and inspect any information	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	To protect confidential or sensitive information, the Compliance Monitoring section of the standard provides that evidence demonstrating compliance with the standard must be retained at the applicable entities' facilities. Additionally, Requirements R2 and R6 require applicable entities to implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged with the~~ made available to third party ~~verifier under Requirement R2~~verifiers and reviewers and to protect or ~~the reviewing entity under Requirement R6. These steps will help ensure that lists of critical facilities or other~~exempt sensitive ~~documents remain~~ or

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
that is needed to ensure compliance with the Reliability Standards.		confidential~~.~~ information developed pursuant to the standard from public disclosure.
11. In addition, the risk assessment used by an owner or operator to identify critical facilities should be verified by an entity other than the owner or operator. Such verification could be performed by NERC, the relevant Regional Entity, a Reliability Coordinator, or another entity. The Reliability Standards should include a procedure for the verifying entity, as well as the Commission, to add or remove facilities from an owner's or operator's list of critical facilities. Similarly, the determination of threats and vulnerabilities and the security plan should also be reviewed by NERC, the relevant Regional Entity, the Reliability Coordinator, or another entity with appropriate expertise. Finally, the Reliability Standards should require that the identification of the critical facilities, the assessment of the potential risks and vulnerabilities, and the security plans be periodically reevaluated and revised to ensure their continued effectiveness. NERC should establish a timeline for when such reevaluations should occur.	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	Requirements R2 and R6 respond to this directive. Under Requirement R3 Transmission Owners must have an unaffiliated ~~entity~~third party verify the risk assessment performed under Requirement R1. The third party verifier must be either (1) a registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or (2) an entity that has transmission planning or analysis experience. The requirement provides that the ~~verifying entity~~verification shall either verify the Transmission Owner's risk assessment or ~~recommend~~include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The verification may occur concurrently with the Requirement R1 risk assessment but must be completed within 90 calendar days of the risk assessment. The Transmission Owner is required to either modify its identification based on the verifier's recommendation or, if it disagrees with the verifier's recommendations, document the technical basis for not modifying its identification. Similarly, under Requirement R6, applicable Transmission Owners and Operators must have an unaffiliated third party review the evaluation performed under Requirement R4 and the

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		security plan(s) developed under Requirement R5. The reviewing entity must be ~~either~~ (1) an entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; (2) an entity or organization approved by the ERO; (3) a governmental agency with physical security expertise; or (4) an entity or organization with demonstrated law enforcement, government, or military physical security expertise. The third party review must be completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The applicable Transmission Owners and Transmission Operators are required to either modify their evaluation or security plan(s) consistent with the reviewer's recommendations or, if they disagree with the recommendations, document the reasons for not modifying. Consistent with the directive to establish a timeline for periodic reevaluation of the identification of facilities that if rendered inoperable or damaged as a result of a physical attack could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection, the assessment of the potential risks and vulnerabilities, and the security plans, the standard provides that Requirement R1 risk assessment should be performed at least once every 30 calendar months for those

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		Transmission Owners that identified facilities in their previous risk assessment and once every 60 calendar months for those Transmission Owners that did not identify facilities in their previous risk assessment. Upon completion of each subsequent risk assessment, the applicable entities must satisfy the obligations under the remaining requirements.
12. Under the Reliability Standards, we anticipate that the number of facilities identified as critical will be relatively small compared to the number of facilities that comprise the Bulk-Power System. For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be "critical" as the term is used in this order. We do not expect that every owner and operator of the Bulk-Power System will have critical facilities under the Reliability Standard. We also recognize that the industry has engaged in longstanding efforts to address the physical security of its critical facilities. Thus, NERC should develop an implementation plan that requires owners or operators of the Bulk-Power System to implement the Reliability Standards in a timely fashion, balancing the importance of protecting the Bulk-Power System from harm while giving the owners or operators adequate time to meaningfully implement the requirements. NERC should file	*Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (Mar. 7, 2014).	The proposed Implementation Plan addresses this directive. As provided in the Implementation Plan, the standard becomes effective the first day of the first calendar quarter that is six months beyond the date that this standard is approved by applicable regulatory authorities or as otherwise provided for in a jurisdiction where approval by an applicable governmental authority is required for a standard to go into effect. This means that the initial risk assessment required by Requirement R1, must be completed on or before the effective date of the standard. The initial performance of Requirements R2 through R6 must be completed according to the timelines specified in those requirements after the effective date of the proposed Reliability Standard, as follows: - Requirement R2, Parts 2.1, 2.2, and 2.4 shall be completed within 90 calendar days of the effective date of the proposed Reliability Standard. Requirement R2, Part 2.3

Project 2014-04 - Physical Security		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
the plan with the Reliability Standards for Commission review.		shall be completed within 60 calendar days of the completion of performance under Requirement R2 part 2.2. - Requirement R3 shall be completed within 7 calendar days of completion of performance under Requirement R2. - Requirements R4 and R5 shall be completed within 120 calendar days of completion of performance under Requirement R2. - Requirement R6, Parts 6.1, 6.2, and 6.4 shall be completed within 90 calendar days of completion of performance under Requirement R5. Requirement R6, Part 6.3 shall be completed within 60 calendar days of Requirement R6 ~~part~~Part 6.2.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2014-04: Physical Security

VRF and VSL Justifications for CIP-014-1

VRF and VSL Justifications – CIP-014-1, R1	
Proposed VRF	High
NERC VRF Discussion	Initial and subsequent risk assessments identify Transmission stations or Transmission substations that need to be assessed for threats and vulnerabilities and potential physical security measures. Since this is a Requirement in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the risk assessment periodicity and the identification of the primary control center that has operational control of Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-002-5.1 R1, which deals with categorizing cyber systems, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner performed an initial risk assessment but did so after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to two calendar months after that date;

VRF and VSL Justifications – CIP-014-1, R1	
	OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 30 calendar months but less than or equal to 32 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 60 calendar months but less than or equal to 62 calendar months.
Proposed Moderate VSL	The Transmission Owner performed an initial risk assessment but did so more than two calendar months after the date specified in the implementation plan for performing the initial risk assessment but less than or equal to four calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 32 calendar months but less than or equal to 34 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 62 calendar months but less than or equal to 64 calendar months.
Proposed High VSL	The Transmission Owner performed an initial risk assessment but did so more than four calendar months after the date specified in

VRF and VSL Justifications – CIP-014-1, R1	
	the implementation plan for performing the initial risk assessment but less than or equal to six calendar months after that date; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 34 calendar months but less than or equal to 36 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after 64 calendar months but less than or equal to 66 calendar months; OR The Transmission Owner performed a risk assessment but failed to include Part 1.2.
Proposed Severe VSL	The Transmission Owner performed an initial risk assessment but did so more than six calendar months after the date specified in the implementation plan for performing the initial risk assessment; OR The Transmission Owner failed to perform an initial risk assessment; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 36 calendar months; OR The Transmission Owner that has identified in its previous risk assessment one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within

VRF and VSL Justifications – CIP-014-1, R1	
	an Interconnection failed to perform a risk assessment; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection performed a subsequent risk assessment but did so after more than 66 calendar months; OR The Transmission Owner that has not identified in its previous risk assessment any Transmission station and Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection failed to perform a subsequent risk assessment.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if the risk assessment is not performed or if the risk assessment is not performed within required intervals.
FERC VSL G3 Violation Severity Level	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R1	
Assignment Should Be Consistent with the Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to submit perform a risk assessment.

VRF and VSL Justifications – CIP-014-1, R2	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party verification of initial and subsequent risk assessments provides reinforcement that the risk assessment was performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party verification including entities that may perform the verification, provisions for adding or removing Transmission stations and/or Transmission substations, and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so in more than 90 calendar days but less than or equal to 100 calendar days following completion of Requirement R1;

VRF and VSL Justifications – CIP-014-1, R2	
	OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 60 calendar days and less than or equal to 70 calendar days from completion of the third party verification.
Proposed Moderate VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 100 calendar days but less than or equal to 110 calendar days following completion of Requirement R1; Or The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 70 calendar days and less than or equal to 80 calendar days from completion of the third party verification.
Proposed High VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 110 calendar days but less than or equal to 120 calendar days following completion of Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 and modified or documented the technical basis for not modifying its identification under Requirement R1 as required by part 2.3 but did so more than 80 calendar days from completion of the third party verification; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to modify or document the technical basis for not modifying its identification under R1 as required by part 2.3.
Proposed Severe VSL	The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but did so more than 120 calendar days following completion of Requirement R1; OR The Transmission Owner failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R2	
	verify the risk assessment performed under Requirement R1; OR The Transmission Owner had an unaffiliated third party verify the risk assessment performed under Requirement R1 but failed to implement procedures for protecting information per Part 2.4.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party verification is not performed or if the verification is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based	The VSL is assigned for a single instance of failing to have an unaffiliated third party verification performed; or failing to perform the verification within prescribe timelines; or failing to implement procedures to protect information.

VRF and VSL Justifications – CIP-014-1, R2	
on A Single Violation, Not on A Cumulative Number of Violations	

VRF and VSL Justifications – CIP-014-1, R3	
Proposed VRF	Lower
NERC VRF Discussion	Notifying the Transmission Operator that it has operational control of a Transmission station or Transmission substation identified in Requirement R1 and verified in Requirement R2 is necessary so that the Transmission Operator may begin performance of subsequent physical security requirements for the primary control center. This is a requirement that is administrative in nature and in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. This justifies a Lower VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the notification of the Transmission Operator regarding the removal of a Transmission station or Transmission substation.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable INT-006-4 R6, which deals with notifying other entities so that Confirmed Interchange may be implemented, is assigned a Lower VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than seven calendar days and less than or equal to nine calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than seven calendar

VRF and VSL Justifications – CIP-014-1, R3	
	days and less than or equal to nine calendar days following the verification or the subsequent risk assessment.
Proposed Moderate VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than nine calendar days and less than or equal to 11 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than nine calendar days and less than or equal to 11 calendar days following the verification or the subsequent risk assessment.
Proposed High VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 11 calendar days and less than or equal to 13 calendar days following the completion of Requirement R2; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 11 calendar days and less than or equal to 13 calendar days following the verification or the subsequent risk assessment.
Proposed Severe VSL	The Transmission Owner notified the Transmission Operator that operates the primary control center as specified in Requirement R3 but did so more than 13 calendar days following the completion of Requirement R2; OR The Transmission Owner failed to notify the Transmission Operator that it operates a control center identified in Requirement R1; OR The Transmission Owner notified the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1 but did so more than 13 calendar days following the verification or the subsequent risk assessment. OR The Transmission Owner failed to notify the Transmission Operator that operates the primary control center of the removal from the identification in Requirement R1.

VRF and VSL Justifications – CIP-014-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if notification is not made subject to the conditions of the requirement.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to make the appropriate notification.

VRF and VSL Justifications – CIP-014-1, R4	
Proposed VRF	Medium
NERC VRF Discussion	Performing an evaluation of potential threats and vulnerabilities of a physical attack to each of respective Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the evaluation of potential threats and vulnerabilities of a physical attack to Transmission stations and/or Transmission substations.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-007-5 R2, which deals with a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets, is assigned a Medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	N/A

VRF and VSL Justifications – CIP-014-1, R4	
Proposed Moderate VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider one of Parts 4.1 through 4.3 in the evaluation.
Proposed High VSL	The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider two of Parts 4.1 through 4.3 in the evaluation.
Proposed Severe VSL	The Responsible Entity failed to conduct an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1; OR The Responsible Entity conducted an evaluation of the potential physical threats and vulnerabilities to each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but failed to consider Parts 4.1 through 4.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failed to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R4	
Severity Level Assignments that Contain Ambiguous Language	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) or failing to consider any of the Requirement Parts 4.1-4.3.

VRF and VSL Justifications – CIP-014-1, R5	
Proposed VRF	High
NERC VRF Discussion	Development, implementation and execution of a documented physical security plan(s) that covers applicable Transmission station(s), Transmission substation(s), and primary control center(s) is necessary to ensure the physical security of those assets as well as the reliability of the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition. This justifies a High VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the physical security plan for applicable Transmission stations, Transmission substations, or primary control centers.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable CIP-003-3 R4, which deals with implementing and documenting a program to identify, classify, and protect information associated with Critical Cyber Assets, is assigned a High VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 120 calendar days but less than or equal to 130 calendar days after completing Requirement R2;

VRF and VSL Justifications – CIP-014-1, R5	
	OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include one of Parts 5.1 through 5.4 in the plan.
Proposed Moderate VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 130 calendar days but less than or equal to 140 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include two of Parts 5.1 through 5.4 in the plan.
Proposed High VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 140 calendar days but less than or equal to 150 calendar days after completing Requirement R2; OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include three of Parts 5.1 through 5.4 in the plan.
Proposed Severe VSL	The Responsible Entity developed and implemented a documented physical security plan(s) that covers each of its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 but did so more than 150 calendar days after completing the verification in Requirement R2; OR The Responsible Entity failed to develop and implement a documented physical security plan(s) that covers its Transmission

VRF and VSL Justifications – CIP-014-1, R5	
	station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1. OR The Responsible Entity developed and implemented a documented physical security plan(s) that covers its Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2 but failed to include Parts 5.1 through 5.4 in the plan.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if a responsible entity fails to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s) or if the responsible entity failed to include any of the Requirement Parts 5.1-5.4.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The language of the VSL directly mirrors the language in the corresponding requirement.
FERC VSL G4 Violation Severity Level	The VSL is assigned for a single instance of failing to develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and

VRF and VSL Justifications – CIP-014-1, R5	
Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	primary control center(s) or failing to include any of the Requirement Parts 5.1-5.4.

VRF and VSL Justifications – CIP-014-1, R6	
Proposed VRF	Medium
NERC VRF Discussion	Unaffiliated third party review of the threat evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 provides reinforcement that these requirements were performed with due consideration to risk to the bulk power system. Since this Requirement is in a planning time frame, a violation could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of this requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition. This justifies a Medium VRF for this requirement.
FERC VRF G1 Discussion	*Guideline 1- Consistency w/ Blackout Report* This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	*Guideline 2- Consistency within a Reliability Standard* The Requirement Parts for this Requirement provide additional detail regarding the unaffiliated third party review including entities that may perform the review, timelines for completing the review and provisions for confidentiality of sensitive information.
FERC VRF G3 Discussion	*Guideline 3- Consistency among Reliability Standards* The comparable EOP-005-2 R6, which deals with verifying that its restoration plan accomplishes its intended function is assigned a medium VRF.
FERC VRF G4 Discussion	*Guideline 4- Consistency with NERC Definitions of VRFs* See "NERC VRF Discussion" above.
FERC VRF G5 Discussion	*Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation* This guideline is not applicable, as the requirement does not co-mingle more than one obligation.
Proposed Lower VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 90 calendar days but less than or equal to 100 calendar days;

VRF and VSL Justifications – CIP-014-1, R6	
	OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 60 calendar days and less than or equal to 70 calendar days following completion of the third party review.
Proposed Moderate VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so in more than 100 calendar days but less than or equal to 110 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 70 calendar days and less than or equal to 80 calendar days following completion of the third party review.
Proposed High VSL	The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did so more than 110 calendar days but less than or equal to 120 calendar days; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 and modified or documented the reason for not modifying the security plan(s) as specified in Part 6.3 but did so more than 80 calendar days following completion of the third party review; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but did not and modify or document the reason for not modifying the security plan(s) as specified in Part 6.3.
Proposed Severe VSL	The Responsible Entity failed to have an unaffiliated third party

VRF and VSL Justifications – CIP-014-1, R6	
	review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 in more than 120 calendar days; OR The Responsible Entity failed to have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5; OR The Responsible Entity had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 but failed to implement procedures for protecting information per Part 6.3.
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	This guideline is not applicable because this is a new requirement.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is not binary. Guideline 2b: The VSL assignment contains clear and unambiguous language that makes clear that the requirement is wholly or partially violated if an unaffiliated third party review is not performed or if the review is not performed within prescribe timelines. The VSLs are also written indicating violation of the Requirement Part regarding protection of information.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the	The language of the VSL directly mirrors the language in the corresponding requirement.

VRF and VSL Justifications – CIP-014-1, R6	
Corresponding Requirement	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	The VSL is assigned for a single instance of failing to have an unaffiliated third party review performed; or failing to perform the review within prescribe timelines; or failing to implement procedures to protect information.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

CIP-014-1 – Physical Security

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC orders, and the language included in this document, FERC orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1												X[3,4]			
R2												X[3,4]			
R3												X[3,4]			
R4												X[3,4]	X[4]		
R5												X[3,4]	X[4]		
R6												X[3,4]	X[4]		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[3] Applicability is further defined to owners of transmission Facilities operated at 500 kV or higher (see section 4.1.1.1 of the Standard) and owners of certain transmission Facilities operating between 200 kV and 499 kV where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations, per section 4.1.1.2 of the Standard. In addition, sections 4.1.1.3 and 4.1.1.4 bring additional transmission Facilities identified as either critical to the derivation of Interconnection Reliability Operating Limits and Nuclear Plant Interface, respectively, within the purview of the standard. Please see the referenced sections of the Standard for additional details regarding applicability of the Requirements to Transmission Owners.

[4] Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Note to Auditors Concerning Third Party Verifications and Reviews

Requirements R2 and R6 prescribe, respectively, unaffiliated third party verifications for Requirement R1 and unaffiliated third party reviews for Requirements R4 and R5. Auditors are encouraged to rely on the verifications and reviews performed in cases where the verifying or reviewing entities are qualified, unaffiliated with the audited entity, and the scope of their verification or review is clear. The concept of reliance means using the work of others to avoid duplication of efforts and is consistent with recognized professional auditing standards, which are required for Compliance Audits per NERC's Rules of Procedure. Reliance in the context of this Reliability Standard means using the Requirement R2 verifications and Requirement R6 reviews to reduce audit risk and the related rigor of audit testing for Requirements R1, R4, and R5. However, in cases where the verifying or reviewing entity lacks the qualifications specified in Requirement R2 for verifications or Requirement R6 for reviewers, the required unaffiliation from the audited entity, or where the scope of the third party entity's verification or review is unclear, auditors may need to apply audit testing of Requirements R1, R4, or R5. For this reason, the Evidence Requested and Compliance Assessment Approach Sections are still present in this RSAW for Requirements R1, R4, and R5. We anticipate those sections will also facilitate expectations for entities and their unaffiliated third party verifiers and reviewers, assist Electric Reliability Organization (ERO) auditors to understand the audit procedures applied by unaffiliated third party verifiers and reviewers, and provide transparency between ERO auditors and Industry, should circumstances require audit testing of Requirements R1, R4, or R5. Further, it is an objective of the ERO to have transparent Evidence Requests and Compliance Assessment Approaches for every enforceable standard, whether they are in audit scope or not.

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1.The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2)one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Registered Entity Response (Required):

Question: Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of Section 4.1.1? ☐ Yes ☐ No

☐ This entity does not have any applicable Transmission stations/substations.

☐ Other: [Provide explanation below]

[Include additional information regarding the question here, including the type of response and format of the response requested, as appropriate.]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R1) Provide the current and the immediately preceding dated risk assessments.
(R1) List of existing Transmission stations/substations that meet the criteria specified in Section 4.1.1.
(R1) List of Transmission stations/substations planned in the next 24 months that meet criteria specified in Section 4.1.1.
(R1 Part 1.2) List of primary control centers that operationally control each identified Transmission station/substation.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R1

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review entity's process for determining Transmission stations/substations subject to identification in accordance with Requirement R1, including weighting described in Section 4.1.1.2.
	(R1) Review entity's risk assessment process to determine the Transmission stations/substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection.
	(R1) Ensure entity's risk assessment process includes Transmission stations/substations planned in the next 24 months.

	(R1) Ensure risk assessment(s) covers each Transmission station/substation meeting applicability described in Section 4.1.
	(R1 Part 1.1) If applicable, review any prior risk assessments and verify whether or not Transmission stations/substations were identified.
	(R1 Part 1.1) Review evidence that risk assessment was performed and verify that it occurred within the past 30 months where items were identified in the previous risk assessment and 60 months where no items were identified in the previous risk assessment.

Note to Auditor: Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary, unless the entity performs the Transmission Operator function for a station/substation meeting the criteria of Requirement R1 Part 1.2.

The 24 month period referenced for Transmission stations/substations planned to be in service is as of the date of the risk assessment not the date of the audit.

See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator;
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification shall verify the Transmission Owner's risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a s Transmission station or Transmission substation::

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated verifying entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R2) Dated evidence of third party verification of the entity's risk assessment performed under Requirement R1.
(R2 Part 2.1) Documented qualifications of the verifying party.
(R2 Part 2.3) Recommendations, if any, of the verifying party related to Requirement R1 risk assessments.
(R2 Part 2.3) Documentation of modifications and implementation of recommendations or technical basis for not implementing recommendations of the verifying party.
(R2 Part 2.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R2) Review evidence of third party verification of the entity's risk assessment and verify the following:
	(R2 Part 2.1) The reviewing entity is registered in accordance with Part 2.1 or has transmission planning or analysis experience.
	(R2 Part 2.2) Verification was completed within 90 calendar days of risk assessment.
	(R2 Part 2.3) Verifying entity's recommendations, if any, were used to modify the entity's Requirement R1 identification or the technical basis for not modifying the Requirement R1 identification is documented within 60 calendar days of completion of the verification.
	(R2 Part 2.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between the entity and third party were implemented.
Note to Auditor See Guidelines and Technical Basis section of the standard and Rationale for Requirement R2 associated with the Standard for additional details regarding the term 'unaffiliated.'	

The third party verification may occur concurrent with or after the risk assessment performed under Requirement R1.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Registered Entity Response (Required):

Question: Are there any primary control centers identified in Requirement R1, Part 1.2 that are not under operational control of your NERC registration? ☐ Yes ☐ No

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R3) If applicable, dated communications with Transmission Operators demonstrating notification and the date of completion of Requirement R2.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R3

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R3) For each applicable primary control center identified in Requirement R1 Part 1.2 not under the control of the entity's registration, verify notification exists and contains the date of completion of Requirement R2.
	(R3 Part 3.1) For each Transmission station/substation removed under Part 3.1, ensure the responsible Transmission Operator was notified of the removal within seven calendar days of removal from identification.
Note to Auditor: Note the entity's response to the above Question. If auditor can verify the entity's answer of 'No,' then Requirement R3 is not applicable and no further audit testing is required.	

Auditor Notes:

.

R4 Supporting Evidence and Documentation

R4. Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R4) A description of the entity's process for executing the evaluation prescribed in Requirement R4.
(R4) Dated evidence of the evaluation prescribed in Requirement R4.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R4

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence of evaluation and verify it considers the following:
	(R4) Potential threats and vulnerabilities as described in Requirement R4.
	(R4 Part 4.1) Unique characteristics as described in Requirement R4 Part 4.1.
	(R4 Part 4.2) Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
	(R4 Part 4.3) Intelligence or warnings as described in Part 4.3.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary control centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 to ensure it is complete.	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R5) Dated physical security plan(s).

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R5

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Review evidence and verify the physical security plan(s) covers the Transmission stations/substations and primary controls identified in Requirements R1 and/or R2, and verify plan was developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). In addition, verify the plan includes the following attributes:
	(R5 Part 5.1) Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.
	(R5 Part 5.2) Law enforcement contact and coordination information.
	(R5 Part 5.3) A timeline for executing physical security enhancements and modifications specified in the physical security plan.
	(R5 Part 5.4) Provisions to evaluate evolving physical threats, and their corresponding security measures in accordance with R5 Part 5.4
	(R5) Verify implementation of physical security plan(s). See 'Note to Auditor' for details.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary control centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities to	

physical attacks per the evaluation conducted in Requirement R4.

Requirement R5 includes implementation of the security plan(s), which is not within the scope of the third party review described in Requirement R6. Auditors can gain reasonable assurance security plan(s) was/were implemented by determining if specific actions prescribed by the plan(s) have taken place within the timelines established by the plan(s). For example, if the plan calls for certain procedures to occur, then auditors could ask for evidence demonstrating the procedure has been implemented within the timeline established in the security plan. Also, if the plan calls for construction of a barrier, an auditor could verify evidence that such a barrier was constructed in accordance with the entity's timeline. As auditors should obtain reasonable, not absolute, assurance the plan(s) was/were implemented, testing implementation on a sample basis may be appropriate.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner identifies a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its security plan(s) consistent with the recommendation; or
- Document the reason for not modifying the security plan(s) consistent with the recommendation

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated reviewing entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security

plan(s) in accordance with a recommendation under Part 6.3. Examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R6) Dated Evidence of unaffiliated third party review of entity's Requirement R4 evaluation and Requirement R5 security plan(s).
(R6 Part 6.1) Evidence that reviewing entity staff meets qualifications identified in Part 6.1.
(R6 Part 6.3) Recommendations of reviewing party related to Requirement R4 evaluation and Requirement R5 security plan.
(R6 Part 6.3) Dated documentation of modifications and implementation of recommendations or reasons and compensating mitigating measures for not implementing recommendations of the reviewing party.
(R6 Part 6.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R6

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R6) Review evidence and verify the physical security plan(s) and the Requirement R4 evaluation have been reviewed by an unaffiliated third party. Also, review evidence and verify the following:
	(R6 Part 6.1) Reviewing party has the qualifications identified in Part 6.1.
	(R6 Part 6.2) Review is dated within 90 calendar days of completion of the Requirement R5 security plan.
	(R6 Part 6.3) Reviewing entity recommended changes to security plan(s) were made by entity or the reason(s) for not making the change(s) was/were documented within 60 calendar days of the completion of the unaffiliated third party review.
	(R6 Part 6.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between entity and third party were implemented.
Note to Auditor: The third party review may occur concurrent with or after the evaluation performed under Requirement R4 or the security plan develop under Requirement R5. See Guidelines and Technical Basis associated with the Standard for additional details related to qualifications of reviewing entities that may inform audited entities selection of a reviewing entity.	

Auditor Notes:

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of CIP-014-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's…….

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's…….

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	04/09/2014	Physical Security RSAW Task Force	New Document
2	05/01/2014	Physical Security RSAW Task Force	Revisions based on comments and changes to the standard.

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

DRAFT Reliability Standard Audit Worksheet[1]

CIP-014-1 – Physical Security

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC orders, and the language included in this document, FERC orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Applicability of Requirements *[RSAW developer to insert correct applicability]*

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1												X[3,4]			
R2												X[3,4]			
R3												X[3,4]			
R4												X[3,4]	X[4]		
R5												X[3,4]	X[4]		
R6												X[3,4]	X[4]		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[3] Applicability is further defined to owners of transmission Facilities operated at 500 kV or higher (see section 4.1.1.1 of the Standard) and owners of certain transmission Facilities operating between 200 kV and 499 kV where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations, per section 4.1.1.2 of the Standard. In addition, sections 4.1.1.3 and 4.1.1.4 bring additional transmission Facilities identified as either critical to the derivation of Interconnection Reliability Operating Limits and Nuclear Plant Interface, respectively, within the purview of the standard. Please see the referenced sections of the Standard for additional details regarding applicability of the Requirements to Transmission Owners.

[4] Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.~~Facilities regulated by the Nuclear Regulatory Commission or Canadian Nuclear Safety Commission are not subject to this Standard.~~

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Note to Auditors Concerning Third Party Verifications and Reviews

Requirements R2 and R6 prescribe, respectively, unaffiliated third party verifications for Requirement R1 and unaffiliated third party reviews for Requirements R4 and R5. Auditors are encouraged to rely on the verifications and reviews performed in cases where the verifying or reviewing entities are qualified, unaffiliated with the audited entity, and the scope of their verification or review is clear. The concept of reliance means using the work of others to avoid duplication of efforts and is consistent with recognized professional auditing standards, which are required for Compliance Audits per NERC's Rules of Procedure. Reliance in the context of this Reliability Standard means using the Requirement R2 verifications and Requirement R6 reviews to reduce audit risk and the related rigor of audit testing for Requirements R1, R4, and R5. However, in cases where the verifying or reviewing entity lacks the qualifications specified in Requirement R2 for verifications or Requirement R6 for reviewers, the required unaffiliation from the audited entity, or where the scope of the third party entity's verification or review is unclear, auditors may need to apply audit testing of Requirements R1, R4, or R5. For this reason, the Evidence Requested and Compliance Assessment Approach Sections are still present in this RSAW for Requirements R1, R4, and R5. We anticipate those sections will also facilitate expectations for entities and their unaffiliated third party verifiers and reviewers, assist Electric Reliability Organization (ERO) auditors to understand the audit procedures applied by unaffiliated third party verifiers and reviewers, and provide transparency between ERO auditors and Industry, should circumstances require audit testing of Requirements R1, R4, or R5. Further, it is an objective of the ERO to have transparent Evidence Requests and Compliance Assessment Approaches for every enforceable standard, whether they are in audit scope or not.

R1 Supporting Evidence and Documentation

R1. Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1.The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify ~~any~~ the Transmission station(s) and Transmission substation(s) that, if rendered inoperable or damaged, could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.1. Subsequent risk assessments shall be performed:

- At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2)one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection; or
- At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, e~~E~~xamples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Registered Entity Response (Required):

Question: ~~As a result of your risk assessment,~~ D~~d~~o you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of Section 4.1.1? ☐ Yes ☐ No

☐ This entity does not have any applicable Transmission stations/substations.

☐ Other: [Provide explanation below]

[Include additional information regarding the question here, including the type of response and format of the response requested, as appropriate.]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R1) Provide the current and the immediately preceding dated risk assessments ~~conducted after the enforceable date of this Standard (i.e. any risk assessments conducted prior to the effective date of this standard are not relevant).~~.
(R1) List of existing Transmission stations/substations that meet the criteria specified in Section 4.1.1.
(R1) List of Transmission stations/substations planned in the next 24 months that meet criteria specified in Section 4.1.1.
(R1 Part 1.2) List of primary control centers that operationally control each identified Transmission station/substation.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R1

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R1) Review entity's process for determining Transmission stations/substations subject to identification in accordance with Requirement R1, including weighting described in Section 4.1.1.2.
	(R1) Review entity's risk assessment process to determine the Transmission stations/substations that if rendered inoperable or damaged could result in widespread instability, uncontrolled separation, or Cascading within an interconnection.

	(R1) Ensure entity's risk assessment process includes Transmission stations/substations planned in the next 24 months.
	(R1) Ensure ~~a~~ risk assessment(s) covers~~was performed for~~ each Transmission station/substation meeting applicability described in Section 4.1.
	(R1 Part 1.1) If applicable, review any prior risk assessments and verify whether or not Transmission stations/substations were identified.
	(R1 Part 1.1) Review evidence that risk assessment was performed and verify that it occurred within the past 30 months where items were identified in the previous risk assessment and 60 months where no items were identified in the previous risk assessment.
Note to Auditor: Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary, unless the entity performs the Transmission Operator function for a station/substation meeting the criteria of Requirement R1 Part 1.2 ~~and no further audit testing of Requirements R3-R6 is necessary~~. The 24 month period referenced for Transmission stations/substations planned to be in service is as of the date of the risk assessment not the date of the audit. **See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.**	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator;
- An entity that has transmission planning or analysis experience.

2.2. The unaffiliated third party verification~~ying entity~~ shall ~~either~~ verify the Transmission Owner's risk assessment performed under Requirement R1, which may include ~~or~~ recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90 calendar days following the completion of the Requirement R1 risk assessment.

2.3. If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a s Transmission station or Transmission substation::

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to ~~exchanged with~~ the unaffiliated verifying entity and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally, e~~E~~xamples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R2) Dated evidence of third party verification of the entity's risk assessment performed under Requirement R1.
(R2 Part 2.1) Documented qualifications of the verifying party.
(R2 Part 2.3) Recommendations, if any, of the verifying party related to Requirement R1 risk assessments.
(R2 Part 2.3) Documentation of modifications and implementation of recommendations or technical basis for not implementing recommendations of the verifying party.
(R2 Part 2.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R2

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R2) Review evidence of third party verification of the entity's risk assessment and verify the following:
	(R2 Part 2.1) The reviewing entity is registered in accordance with Part 2.1 or has transmission planning or analysis experience.
	(R2 Part 2.2) Verification was completed within 90 calendar days of risk assessment.
	(R2 Part 2.3) Verifying entity's recommendations, if any, were used to modify the entity's Requirement R1 identification or the technical basis for not modifying the Requirement R1 identification is documented within 60 calendar days of completion of the verification.
	(R2 Part 2.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between the entity and third party were implemented.
Note to Auditor See Guidelines and Technical Basis section of the standard and Rationale for Requirement R2 associated with the Standard for additional details regarding the term 'unaffiliated.'	

The third party verification may occur concurrent with or after the risk assessment performed under Requirement R1.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. For ~~a~~the primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation ~~and~~ verified according to Requirement R2, and b) ~~that~~ is not under the operational control of the Transmission Owner, the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the primary control center of such identification and the date of completion of Requirement R2.

3.1. If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Registered Entity Response (Required):

Question: Are there any primary control centers identified in Requirement R1, Part 1.2 that are not under operational control of your NERC registration? ☐ Yes ☐ No

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R3) If applicable, dated communications with Transmission Operators demonstrating notification and the date of completion of Requirement R2.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R3

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R3) For each applicable primary control center identified in Requirement R1 Part 1.2 not under the control of the entity's registration, verify notification exists and contains the date of completion of Requirement R2.
	(R3 Part 3.1) For each Transmission station/substation removed under Part 3.1, ensure the responsible Transmission Operator was notified of the removal within seven calendar days of removal from identification.
Note to Auditor: Note the entity's response to the above Question. If auditor can verify the entity's answer of 'No,' then Requirement R3 is not applicable and no further audit testing is required.	

Auditor Notes:

.

R4 Supporting Evidence and Documentation

R4. Each Transmission Owner that ~~owns or operates~~ identified a Transmission station, Transmission substation, or a primary control center ~~identified~~ in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:

4.1. Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);

4.2. Prior history of ~~f~~ attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and

4.3. Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R4) A description of the entity's process for executing the evaluation prescribed in Requirement R4.
(R4) Dated evidence of the evaluation prescribed in Requirement R4.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R4

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R4) Review evidence of evaluation and verify it considers the following:
	(R4) Potential threats and vulnerabilities as described in Requirement R4.
	(R4 Part 4.1) Unique characteristics as described in Requirement R4 Part 4.1.
	(R4 Part 4.2) Prior history of ~~r~~ attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
	(R4 Part 4.3) Intelligence or warnings as described in Part 4.3.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary c~~C~~ontrol c~~C~~enters identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 to ensure it is complete.	

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner that identified ~~owns or has operational control of~~ a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for ~~implementing~~ executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating ~~implementation~~ execution of the physical security plan according to the timeline specified in the physical security plan.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R5) Dated physical security plan(s).

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R5

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R5) Review evidence and verify the physical security plan(s) covers the Transmission stations/substations and primary controls identified in Requirements R1 and/or R2, and verify plan was ~~implemented~~ developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). In addition, verify the plan includes the following attributes:
	(R5 Part 5.1) Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities ~~based on the results of~~identified during the evaluation conducted in Requirement R4.
	(R5 Part 5.2) Law enforcement contact and coordination information.
	(R5 Part 5.3) A timeline for ~~implementing~~ executing physical security enhancements and modifications specified in the physical security plan.
	(R5 Part 5.4) Provisions to evaluate evolving physical threats, and their corresponding security measures in accordance with R5 Part 5.4
	(R5) Verify implementation of physical security plan(s). See 'Note to Auditor' for details.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary c~~C~~ontrol c~~C~~enters	

identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities ~~that would facilitate~~to physical attacks ~~that have a high probability or likelihood of occurrence~~per the evaluation conducted in Requirement R4.

Requirement R5 includes implementation of the security plan(s), which is not within the scope of the third party review described in Requirement R6. Auditors can gain reasonable assurance security plan(s) was/were implemented by determining if specific actions prescribed by the plan(s) have taken place within the timelines established by the plan(s). For example, if the plan calls for certain procedures to occur, then auditors could ask for evidence demonstrating the procedure has been implemented within the timeline established in the security plan. Also, if the plan calls for construction of a barrier, an auditor could verify evidence that such a barrier was constructed in accordance with the entity's timeline. As auditors should obtain reasonable, not absolute, assurance the plan(s) was/were implemented, testing implementation on a sample basis may be appropriate.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner ~~that owns or operates~~identifies a Transmission station, Transmission substation, or primary control center identified in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3 ~~that the Transmission Operator's primary control center has operational control of an identified Transmission station or Transmission substation~~, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.

6.3. If the unaffiliated third party reviewer~~ing entity~~ recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:

- Modify its security plan(s) consistent with the recommendation; or
- Document the reason for not modifying the security plan(s) consistent with the recommendation

6.4. Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information ~~exchanged~~ made available to ~~with~~ the unaffiliated reviewing entity ~~and from any other form of public disclosure~~ and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation

performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security plan(s) in accordance with a recommendation under Part 6.3. Examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R6) Dated Evidence of unaffiliated third party review of entity's Requirement R4 evaluation and Requirement R5 security plan(s).
(R6 Part 6.1) Evidence that reviewing entity staff meets qualifications identified in Part 6.1.
(R6 Part 6.3) Recommendations of reviewing party related to Requirement R4 evaluation and Requirement R5 security plan.
(R6 Part 6.3) Dated documentation of modifications and implementation of recommendations or reasons and compensating mitigating measures for not implementing recommendations of the reviewing party.
(R6 Part 6.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-1, R6

This section to be completed by the Compliance Enforcement Authority

	The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.
	(R6) Review evidence and verify the physical security plan(s) and the Requirement R4 evaluation have been reviewed by an unaffiliated third party. Also, review evidence and verify the following:
	(R6 Part 6.1) Reviewing party has the qualifications identified in Part 6.1.
	(R6 Part 6.2) Review is dated within 90 calendar days of completion of the Requirement R5 security plan.
	(R6 Part 6.3) Reviewing entity recommended changes to security plan(s) were made by entity or the reason(s) for not making the change(s) was/were documented within 60 calendar days of the completion of the unaffiliated third party review.
	(R6 Part 6.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between entity and third party were implemented.
Note to Auditor: The third party review may occur concurrent with or after the evaluation performed under Requirement R4 or the security plan develop under Requirement R5. See Guidelines and Technical Basis associated with the Standard for additional details related to qualifications of reviewing entities that may inform audited entities selection of a reviewing entity.	

Auditor Notes:

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of CIP-014-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's…….

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's…….

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	04/09/2014	Physical Security RSAW Task Force	New Document
2	05~~4~~/01~~XX~~/2014	Physical Security RSAW Task Force	Revisions based on comments and changes to the standard.

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Final Ballot Now Open through May 5, 2014

Now Available

A final ballot of **CIP-014-1 – Physical Security** is now open through **8 p.m. Eastern on Monday, May 5, 2014.**

In an order issued March 7, 2014, the Federal Energy Regulatory Commission directed NERC to file a physical security standard within 90 days of the order (i.e. by June 5, 2014). On March 21, 2014, the NERC Standards Committee (SC) authorized a waiver of the standard development process, in accordance with Section 16 of the Standard Processes Manual, to meet this pending regulatory deadline. The SC approved to shorten this final ballot period from 10 days to 5 calendar days. (Section 4.9)

If you have questions please contact Stephen Crutchfield via email or by telephone at (609) 651-9455. Background information for this project can be found on the project page.

Instructions for Balloting

In the final ballot, votes are counted by exception. Only members of the ballot pool may cast a ballot; all ballot pool members may change their previously cast votes. A ballot pool member who failed to cast a ballot during the last ballot window may cast a ballot in the final ballot window. If a ballot pool member does not participate in the final ballot, that member's vote cast in the previous ballot will be carried over as that member's vote in the final ballot.

Members of the ballot pool associated with this project may log in and submit their vote for the standard by clicking here.

Next Steps

Voting results for the standard will be posted and announced after the ballot window closes. If approved, it will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For more information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller, Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2014-04 Physical Security
CIP-014-1

Final Ballot Results

Now Available

A final ballot for **CIP-014-1 – Physical Security** concluded at **8 p.m. Eastern on Monday, May 5, 2014.**

The standard achieved a quorum and sufficient affirmative votes for approval. Voting statistics are listed below, and the Ballot Results page provides a link to the detailed results for the ballot.

Standard	Quorum / Approval
CIP-014-1	92.53% / 85.61%

Background information for this project can be found on the project page.

Next Steps
The standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

For information on the **Standards Development Process**, please refer to the Standard Processes Manual.

For more information or assistance, please contact Wendy Muller (via email), Standards Development Administrator, or at 404-446-2560.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Ballot Results	
Ballot Name:	2014-04_Physical_Security_CIP-014-1
Ballot Period:	5/1/2014 - 5/5/2014
Ballot Type:	Final
Total # Votes:	421
Total Ballot Pool:	455
Quorum:	**92.53 % The Quorum has been reached**
Weighted Segment Vote:	85.61 %
Ballot Results:	**A quorum was reached and there were sufficient affirmative votes for approval.**

Summary of Ballot Results

Segment	Ballot Pool	Segment Weight	Affirmative # Votes	Affirmative Fraction	Negative # Votes	Negative Fraction	Negative Vote without a Comment	Abstain	No Vote
1 - Segment 1	121	1	97	0.858	16	0.142	0	3	5
2 - Segment 2	8	0.6	6	0.6	0	0	0	1	1
3 - Segment 3	104	1	85	0.924	7	0.076	0	4	8
4 - Segment 4	38	1	31	0.912	3	0.088	0	1	3
5 - Segment 5	101	1	76	0.905	8	0.095	0	5	12
6 - Segment 6	60	1	55	0.965	2	0.035	0	1	2
7 - Segment 7	5	0.3	3	0.3	0	0	0	0	2
8 - Segment 8	6	0.6	2	0.2	4	0.4	0	0	0
9 - Segment 9	3	0.1	1	0.1	0	0	0	2	0

10 - Segment 10	9	0.6	4	0.4	2	0.2	0	2	1
Totals	**455**	**7.2**	**360**	**6.164**	**42**	**1.036**	**0**	**19**	**34**

Individual Ballot Pool Results

Segment	Organization	Member	Ballot	NERC Notes
1	Ameren Services	Eric Scott	Affirmative	
1	American Electric Power	Paul B Johnson	Affirmative	
1	American Transmission Company, LLC	Andrew Z Pusztai	Affirmative	
1	Arizona Public Service Co.	Robert Smith	Affirmative	
1	Associated Electric Cooperative, Inc.	John Bussman	Affirmative	
1	ATCO Electric	Glen Sutton	Affirmative	
1	Austin Energy	James Armke		
1	Avista Utilities	Heather Rosentrater	Affirmative	
1	Balancing Authority of Northern California	Kevin Smith	Affirmative	
1	Baltimore Gas & Electric Company	Christopher J Scanlon	Affirmative	
1	Basin Electric Power Cooperative	David Rudolph	Affirmative	
1	BC Hydro and Power Authority	Patricia Robertson	Abstain	
1	Black Hills Corp	Wes Wingen	Negative	COMMENT RECEIVED
1	Bonneville Power Administration	Donald S. Watkins	Affirmative	
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey	Affirmative	
1	Bryan Texas Utilities	John C Fontenot	Affirmative	
1	CenterPoint Energy Houston Electric, LLC	John Brockhan	Affirmative	
1	Central Electric Power Cooperative	Michael B Bax	Affirmative	
1	Central Hudson Gas & Electric Corp.	Frank Pace	Negative	
1	Central Iowa Power Cooperative	Kevin J Lyons	Affirmative	
1	Central Maine Power Company	Joseph Turano Jr.	Affirmative	
1	City of Garland	David Grubbs	Affirmative	
1	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	Chang G Choi	Affirmative	
1	City of Tallahassee	Daniel S Langston	Affirmative	
1	Clark Public Utilities	Jack Stamper	Affirmative	
1	Cleco Power LLC	Danny McDaniel	Affirmative	
1	Colorado Springs Utilities	Shawna Speer	Affirmative	
1	Consolidated Edison Co. of New York	Christopher L de Graffenried	Affirmative	
1	CPS Energy	Glenn Pressler	Affirmative	
1	Deseret Power	James Tucker		
1	Dominion Virginia Power	Larry Nash	Affirmative	
1	Duke Energy Carolina	Doug E Hils	Affirmative	
1	East Kentucky Power Coop.	Amber Anderson	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Edison Electric Institute	David Batz	Affirmative	
1	El Paso Electric Company	Pablo Onate	Affirmative	
1	Empire District Electric Co.	Ralph F Meyer	Affirmative	
1	Encari	Steven E Hamburg	Negative	COMMENT RECEIVED
1	Entergy Transmission	Oliver A Burke	Affirmative	
1	FirstEnergy Corp.	William J Smith	Affirmative	
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton	Negative	
1	Florida Power & Light Co.	Mike O'Neil	Affirmative	
1	FortisBC	Curtis Klashinsky	Affirmative	
1	Gainesville Regional Utilities	Richard Bachmeier	Affirmative	
1	Georgia Transmission Corporation	Jason Snodgrass	Affirmative	
1	Great River Energy	Gordon Pietsch	Affirmative	
1	Hoosier Energy Rural Electric Cooperative, Inc.	Bob Solomon		
1	Hydro-Quebec TransEnergie	Martin Boisvert	Negative	
1	Idaho Power Company	Molly Devine	Negative	
1	International Transmission Company Holdings Corp	Michael Moltane	Negative	
1	JDRJC Associates	Jim D Cyrulewski	Affirmative	

1	JEA	Ted Hobson	Affirmative	
1	KAMO Electric Cooperative	Walter Kenyon	Affirmative	
1	Kansas City Power & Light Co.	Daniel Gibson	Affirmative	
1	Lakeland Electric	Larry E Watt	Affirmative	
1	Lee County Electric Cooperative	John Chin	Abstain	
1	Lincoln Electric System	Doug Bantam	Affirmative	
1	Los Angeles Department of Water & Power	John Burnett	Affirmative	
1	Lower Colorado River Authority	Martyn Turner	Affirmative	
1	M & A Electric Power Cooperative	William Price	Affirmative	
1	Manitoba Hydro	Nazra S Gladu	Affirmative	COMMENT RECEIVED
1	MEAG Power	Danny Dees	Affirmative	
1	MidAmerican Energy Co.	Terry Harbour	Affirmative	
1	Minnesota Power, Inc.	Randi K. Nyholm	Affirmative	
1	Minnkota Power Coop. Inc.	Daniel L Inman	Affirmative	
1	Muscatine Power & Water	Andrew J Kurriger		
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey	Affirmative	
1	National Grid USA	Michael Jones	Affirmative	
1	NB Power Corporation	Alan MacNaughton	Negative	
1	Network & Security Technologies	Nicholas Lauriat	Abstain	
1	New York Power Authority	Bruce Metruck	Affirmative	
1	North Carolina Electric Membership Corp.	Robert Thompson	Affirmative	
1	Northeast Missouri Electric Power Cooperative	Kevin White	Affirmative	
1	Northeast Utilities	William Temple	Affirmative	
1	Northern Indiana Public Service Co.	Julaine Dyke	Affirmative	
1	NorthWestern Energy	John Canavan	Affirmative	
1	Ohio Valley Electric Corp.	Scott R Cunningham	Affirmative	
1	Oklahoma Gas and Electric Co.	Terri Pyle	Affirmative	
1	Omaha Public Power District	Doug Peterchuck	Negative	
1	Oncor Electric Delivery	Jen Fiegel	Affirmative	
1	Orlando Utilities Commission	Brad Chase	Affirmative	
1	Otter Tail Power Company	Daryl Hanson	Affirmative	
1	Pacific Gas and Electric Company	Bangalore Vijayraghavan	Affirmative	
1	Peak Reliability	Jared Shakespeare	Negative	
1	Platte River Power Authority	John C. Collins	Affirmative	
1	Portland General Electric Co.	John T Walker	Affirmative	
1	Potomac Electric Power Co.	David Thorne	Affirmative	
1	PPL Electric Utilities Corp.	Brenda L Truhe	Affirmative	
1	Public Service Company of New Mexico	Laurie Williams	Affirmative	
1	Public Service Electric and Gas Co.	Kenneth D. Brown	Affirmative	
1	Public Utility District No. 1 of Chelan County	Chad Bowman	Affirmative	
1	Public Utility District No. 1 of Okanogan County	Dale Dunckel		
1	Puget Sound Energy, Inc.	Denise M Lietz	Affirmative	
1	Rochester Gas and Electric Corp.	John C. Allen	Affirmative	
1	Sacramento Municipal Utility District	Tim Kelley	Affirmative	
1	Salt River Project	Robert Kondziolka	Affirmative	
1	San Diego Gas & Electric	Will Speer	Affirmative	
1	Seattle City Light	Pawel Krupa	Negative	
1	Seminole Electric Cooperative, Inc.	Glenn Spurlock	Affirmative	
1	Sho-Me Power Electric Cooperative	Denise Stevens	Affirmative	
1	Snohomish County PUD No. 1	Long T Duong	Affirmative	
1	South Carolina Electric & Gas Co.	Tom Hanzlik	Affirmative	
1	South Carolina Public Service Authority	Shawn T Abrams	Affirmative	
1	Southern California Edison Company	Steven Mavis	Affirmative	
1	Southern Company Services, Inc.	Robert A. Schaffeld	Affirmative	
1	Southern Illinois Power Coop.	William Hutchison	Negative	
1	Southern Indiana Gas and Electric Co.	Lynnae Wilson	Affirmative	
1	Southwest Transmission Cooperative, Inc.	John Shaver	Negative	SUPPORTS THIRD PARTY COMMENTS
1	Southwestern Power Administration	Angela L Summer	Affirmative	
1	Sunflower Electric Power Corporation	Noman Lee Williams	Affirmative	
1	Tampa Electric Co.	Beth Young	Affirmative	
1	Tennessee Valley Authority	Howell D Scott	Negative	
1	Trans Bay Cable LLC	Steven Powell	Affirmative	
1	Transmission Agency of Northern California	Bryan Griess	Affirmative	

1	Tri-State Generation & Transmission Association, Inc.	Tracy Sliman	Negative	COMMENT RECEIVED
1	Tucson Electric Power Co.	John Tolo	Affirmative	
1	U.S. Bureau of Reclamation	Richard T Jackson	Affirmative	
1	United Illuminating Co.	Jonathan Appelbaum	Affirmative	
1	Vermont Electric Power Company, Inc.	Kim Moulton	Affirmative	
1	Westar Energy	Allen Klassen	Affirmative	
1	Western Area Power Administration	Lloyd A Linke	Affirmative	
1	Xcel Energy, Inc.	Gregory L Pieper	Affirmative	
2	BC Hydro	Venkataramakrishnan Vinnakota	Abstain	
2	California ISO	Rich Vine	Affirmative	
2	Electric Reliability Council of Texas, Inc.	Cheryl Moseley	Affirmative	
2	Independent Electricity System Operator	Barbara Constantinescu	Affirmative	
2	MISO	Marie Knox	Affirmative	
2	New York Independent System Operator	Gregory Campoli	Affirmative	
2	PJM Interconnection, L.L.C.	stephanie monzon	Affirmative	
2	Southwest Power Pool, Inc.	Charles H. Yeung		
3	AEP	Michael E Deloach	Affirmative	
3	Alabama Power Company	Robert S Moore	Affirmative	
3	American Public Power Association	Nathan Mitchell	Affirmative	
3	APS	Sarah Kist	Affirmative	
3	Arkansas Electric Cooperative Corporation	Philip Huff	Affirmative	
3	Associated Electric Cooperative, Inc.	Todd Bennett	Affirmative	
3	Atlantic City Electric Company	NICOLE BUCKMAN	Affirmative	
3	Avista Corp.	Scott J Kinney	Affirmative	
3	BC Hydro and Power Authority	Pat G. Harrington	Abstain	
3	Blue Ridge Electric	James L Layton		
3	Bonneville Power Administration	Rebecca Berdahl	Affirmative	
3	Central Electric Power Cooperative	Adam M Weber	Affirmative	
3	Central Hudson Gas & Electric Corp.	James J McCloskey		
3	City of Anaheim Public Utilities Department	Dennis M Schmidt	Abstain	
3	City of Austin dba Austin Energy	Andrew Gallo	Affirmative	
3	City of Clewiston	Lynne Mila	Affirmative	
3	City of Farmington	Linda R Jacobson	Affirmative	
3	City of Garland	Ronnie C Hoeinghaus	Affirmative	
3	City of Green Cove Springs	Mark Schultz	Abstain	
3	City of Redding	Bill Hughes	Affirmative	
3	City of Tallahassee	Bill R Fowler	Affirmative	
3	Cleco Corporation	Michelle A Corley	Affirmative	
3	Colorado Springs Utilities	Jean Mueller	Affirmative	
3	ComEd	John Bee	Affirmative	
3	Consolidated Edison Co. of New York	Peter T Yost	Affirmative	
3	Consumers Energy Company	Gerald G Farringer	Affirmative	
3	Cowlitz County PUD	Russell A Noble	Negative	COMMENT RECEIVED
3	CPS Energy	Jose Escamilla	Affirmative	
3	Dayton Power & Light Co.	Jeffrey Fuller	Negative	
3	Delmarva Power & Light Co.	Michael R. Mayer	Affirmative	
3	Dominion Resources, Inc.	Connie B Lowe	Affirmative	
3	DTE Electric	Kent Kujala	Affirmative	
3	East Kentucky Power Coop.	Patrick Woods	Negative	SUPPORTS THIRD PARTY COMMENTS
3	El Paso Electric Company	Rhonda Bryant	Affirmative	
3	Empire District Electric Co.	Kalem Long	Affirmative	
3	Entergy	Kevin Weber	Affirmative	
3	FirstEnergy Corp.	Cindy E Stewart	Affirmative	
3	Florida Keys Electric Cooperative	Tom B Anthony	Negative	
3	Florida Municipal Power Agency	Joe McKinney	Affirmative	
3	Florida Power & Light Co.	Summer C. Esquerre	Affirmative	
3	Florida Power Corporation	Lee Schuster	Affirmative	
3	Gainesville Regional Utilities	Kenneth Simmons	Affirmative	
3	Georgia System Operations Corporation	Scott McGough	Affirmative	
3	Great River Energy	Brian Glover		
3	Hydro One Networks, Inc.	Ayesha Sabouba	Affirmative	
3	Imperial Irrigation District	Jesus S. Alcaraz		

3	JEA	Garry Baker	Affirmative	
3	KAMO Electric Cooperative	Theodore J Hilmes		
3	Kansas City Power & Light Co.	Joshua D Bach	Affirmative	
3	Kissimmee Utility Authority	Gregory D Woessner	Affirmative	
3	Lakeland Electric	Mace D Hunter	Affirmative	
3	Lee County Electric Cooperative	David A Hadzima		
3	Lincoln Electric System	Jason Fortik	Affirmative	
3	Los Angeles Department of Water & Power	Mike Anctil		
3	Louisville Gas and Electric Co.	Charles A. Freibert	Affirmative	
3	M & A Electric Power Cooperative	Stephen D Pogue	Affirmative	
3	Manitoba Hydro	Greg C. Parent	Affirmative	
3	MEAG Power	Roger Brand	Affirmative	
3	MidAmerican Energy Co.	Thomas C. Mielnik	Affirmative	
3	Modesto Irrigation District	Jack W Savage	Affirmative	
3	Muscatine Power & Water	John S Bos	Affirmative	
3	National Grid USA	Brian E Shanahan	Affirmative	
3	National Rural Electric Cooperative Association	Patricia E Metro	Affirmative	
3	Nebraska Public Power District	Tony Eddleman	Affirmative	
3	New York Power Authority	David R Rivera	Affirmative	
3	North Carolina Electric Membership Corp.	Doug White	Affirmative	
3	North Carolina Municipal Power Agency #1	Kathy Moyer	Affirmative	
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann	Affirmative	
3	Northern Indiana Public Service Co.	Ramon J Barany	Affirmative	
3	NRG Energy Power Marketing, Inc.	Rick Keetch	Affirmative	
3	NW Electric Power Cooperative, Inc.	David McDowell	Affirmative	
3	Ocala Utility Services	Randy Hahn	Affirmative	
3	Oklahoma Gas and Electric Co.	Donald Hargrove	Affirmative	
3	Omaha Public Power District	Blaine R. Dinwiddie	Affirmative	
3	Orlando Utilities Commission	Ballard K Mutters	Affirmative	
3	Owensboro Municipal Utilities	Thomas T Lyons	Affirmative	
3	Pacific Gas and Electric Company	John H Hagen	Affirmative	
3	Platte River Power Authority	Terry L Baker	Affirmative	
3	PNM Resources	Michael Mertz	Affirmative	
3	Portland General Electric Co.	Thomas G Ward	Affirmative	
3	Potomac Electric Power Co.	Mark Yerger	Affirmative	
3	Public Service Electric and Gas Co.	Jeffrey Mueller	Affirmative	
3	Public Utility District No. 1 of Chelan County	Steve Wickel	Affirmative	
3	Public Utility District No. 1 of Clallam County	Doug Adams	Affirmative	
3	Puget Sound Energy, Inc.	Mariah R Kennedy	Affirmative	
3	Rutherford EMC	Thomas Haire	Abstain	
3	Sacramento Municipal Utility District	James Leigh-Kendall	Affirmative	
3	Salt River Project	John T. Underhill	Affirmative	
3	Santee Cooper	James M Poston	Affirmative	
3	Seattle City Light	Dana Wheelock	Negative	
3	Seminole Electric Cooperative, Inc.	James R Frauen	Affirmative	
3	Sho-Me Power Electric Cooperative	Jeff L Neas	Affirmative	
3	Snohomish County PUD No. 1	Mark Oens	Affirmative	
3	South Carolina Electric & Gas Co.	Hubert C Young	Affirmative	
3	Southern California Edison Company	Lujuanna Medina	Affirmative	
3	Southern Indiana Gas and Electric Co.	Fred Frederick	Affirmative	
3	Tacoma Power	Marc Donaldson	Affirmative	
3	Tampa Electric Co.	Ronald L. Donahey	Affirmative	
3	Tennessee Valley Authority	Ian S Grant	Negative	
3	Tri-State Generation & Transmission Association, Inc.	Janelle Marriott	Negative	
3	Westar Energy	Bo Jones	Affirmative	
3	Wisconsin Electric Power Marketing	James R Keller	Affirmative	
3	Wisconsin Public Service Corp.	Gregory J Le Grave		
3	Xcel Energy, Inc.	Michael Ibold	Affirmative	
4	Alliant Energy Corp. Services, Inc.	Kenneth Goldsmith	Affirmative	
4	Arkansas Electric Cooperative Corporation	Ronnie Frizzell	Affirmative	
4	Blue Ridge Power Agency	Duane S Dahlquist	Affirmative	
4	City of Austin dba Austin Energy	Reza Ebrahimian	Affirmative	
4	City of Redding	Nicholas Zettel	Affirmative	
4	City Utilities of Springfield, Missouri	John Allen	Affirmative	
4	Constellation Energy Control & Dispatch, L.L.C.	Margaret Powell	Affirmative	

4	Consumers Energy Company	Tracy Goble	Affirmative	
4	Cowlitz County PUD	Rick Syring	Negative	COMMENT RECEIVED
4	DTE Electric	Daniel Herring	Affirmative	
4	Eugene Water & Electric Board	Dean Ahlsten	Affirmative	
4	Flathead Electric Cooperative	Russ Schneider	Negative	COMMENT RECEIVED
4	Florida Municipal Power Agency	Frank Gaffney	Affirmative	
4	Fort Pierce Utilities Authority	Cairo Vanegas	Affirmative	
4	Garkane Energy	Mike Avant		
4	Georgia System Operations Corporation	Guy Andrews	Affirmative	
4	Herb Schrayshuen	Herb Schrayshuen	Affirmative	
4	Illinois Municipal Electric Agency	Bob C. Thomas	Affirmative	
4	Indiana Municipal Power Agency	Jack Alvey	Abstain	
4	Integrys Energy Group, Inc.	Christopher Plante	Affirmative	
4	LaGen	Richard Comeaux	Affirmative	
4	Madison Gas and Electric Co.	Joseph DePoorter	Affirmative	
4	Modesto Irrigation District	Spencer Tacke	Affirmative	
4	National Rural Electric Cooperative Association	Barry R. Lawson	Affirmative	
4	North Carolina Electric Membership Corp.	John Lemire	Affirmative	
4	Ohio Edison Company	Douglas Hohlbaugh	Affirmative	
4	Oklahoma Municipal Power Authority	Ashley Stringer	Affirmative	
4	Old Dominion Electric Coop.	Mark Ringhausen	Affirmative	
4	Public Utility District No. 1 of Douglas County	Henry E. LuBean		
4	Public Utility District No. 1 of Snohomish County	John D Martinsen	Affirmative	
4	Sacramento Municipal Utility District	Mike Ramirez	Affirmative	
4	Seattle City Light	Hao Li	Negative	
4	Seminole Electric Cooperative, Inc.	Steven R Wallace	Affirmative	
4	South Mississippi Electric Power Association	Steve McElhaney	Affirmative	
4	Southern Minnesota Municipal Power Agency	Richard L Koch		
4	Tacoma Public Utilities	Keith Morisette	Affirmative	
4	Utility Services, Inc.	Brian Evans-Mongeon	Affirmative	
4	Wisconsin Energy Corp.	Anthony Jankowski	Affirmative	
5	Acciona Energy North America	George E Brown	Abstain	
5	Amerenue	Sam Dwyer	Affirmative	
5	American Electric Power	Thomas Foltz	Affirmative	
5	Arizona Public Service Co.	Scott Takinen	Affirmative	
5	Associated Electric Cooperative, Inc.	Matthew Pacobit		
5	Avista Corp.	Steve Wenke		
5	BC Hydro and Power Authority	Clement Ma	Abstain	
5	Black Hills Corp	George Tatar	Negative	
5	Boise-Kuna Irrigation District/dba Lucky peak power plant project	Mike D Kukla	Negative	
5	Bonneville Power Administration	Francis J. Halpin	Affirmative	
5	BP Wind Energy North America Inc	Carla Holly	Affirmative	
5	Brazos Electric Power Cooperative, Inc.	Shari Heino	Affirmative	
5	Calpine Corporation	Hamid Zakery	Abstain	
5	City and County of San Francisco	Daniel Mason	Affirmative	
5	City of Austin dba Austin Energy	Jeanie Doty	Affirmative	
5	City of Redding	Paul A. Cummings	Affirmative	
5	City of Tallahassee	Karen Webb	Affirmative	
5	City Water, Light & Power of Springfield	Steve Rose	Affirmative	
5	Cleco Power	Stephanie Huffman	Affirmative	
5	Cogentrix Energy Power Management, LLC	Mike D Hirst	Abstain	
5	Colorado Springs Utilities	Kaleb Brimhall	Affirmative	
5	Con Edison Company of New York	Brian O'Boyle	Affirmative	
5	Consumers Energy Company	David C Greyerbiehl	Affirmative	
5	Cowlitz County PUD	Bob Essex	Negative	COMMENT RECEIVED
5	CPS Energy	Robert Stevens	Affirmative	
5	Dairyland Power Coop.	Tommy Drea		
5	Dominion Resources, Inc.	Mike Garton	Affirmative	
5	DTE Electric	Mark Stefaniak	Affirmative	
5	Duke Energy	Dale Q Goodwine	Affirmative	
5	Dynegy Inc.	Dan Roethemeyer	Affirmative	
5	E.ON Climate & Renewables North America, LLC	Dana Showalter	Abstain	

5	East Kentucky Power Coop.	Stephen Ricker	Negative	SUPPORTS THIRD PARTY COMMENTS
5	El Paso Electric Company	Gustavo Estrada	Affirmative	
5	Electric Power Supply Association	John R Cashin		
5	Empire District Electric Co.	mike l kidwell	Affirmative	
5	Entergy Services, Inc.	Tracey Stubbs	Affirmative	
5	Exelon Nuclear	Mark F Draper	Affirmative	
5	First Wind	John Robertson	Affirmative	
5	FirstEnergy Solutions	Kenneth Dresner	Affirmative	
5	Florida Municipal Power Agency	David Schumann	Affirmative	
5	Great River Energy	Preston L Walsh	Negative	SUPPORTS THIRD PARTY COMMENTS
5	Hydro-Québec Production	Roger Dufresne	Negative	
5	Ingleside Cogeneration LP	Michelle R DAntuono	Affirmative	
5	JEA	John J Babik	Affirmative	
5	Kansas City Power & Light Co.	Brett Holland	Affirmative	
5	Kissimmee Utility Authority	Mike Blough	Affirmative	
5	Lafayette Utilities System	Jamie B Webb		
5	Lakeland Electric	James M Howard	Affirmative	
5	Liberty Electric Power LLC	Daniel Duff		
5	Lincoln Electric System	Dennis Florom	Affirmative	
5	Los Angeles Department of Water & Power	Kenneth Silver	Affirmative	
5	Lower Colorado River Authority	Dixie Wells	Affirmative	
5	Manitoba Hydro	Chris Mazur	Affirmative	
5	Massachusetts Municipal Wholesale Electric Company	David Gordon	Affirmative	
5	MEAG Power	Steven Grego	Affirmative	
5	Muscatine Power & Water	Mike Avesing	Affirmative	
5	Nebraska Public Power District	Don Schmit	Affirmative	
5	Nevada Power Co.	Richard Salgo	Affirmative	
5	New York Power Authority	Wayne Sipperly	Affirmative	
5	NextEra Energy	Allen D Schriver	Affirmative	
5	North Carolina Electric Membership Corp.	Jeffrey S Brame	Affirmative	
5	Northern Indiana Public Service Co.	Michael D Melvin	Affirmative	
5	Oglethorpe Power Corporation	Bernard Johnson	Affirmative	
5	Oklahoma Gas and Electric Co.	Henry L Staples	Affirmative	
5	Omaha Public Power District	Mahmood Z. Safi	Affirmative	
5	Ontario Power Generation Inc.	David Ramkalawan	Affirmative	
5	Orlando Utilities Commission	Richard K Kinas	Affirmative	
5	Pacific Gas and Electric Company	Alex Chua	Affirmative	
5	Platte River Power Authority	Christopher R Wood	Affirmative	
5	Portland General Electric Co.	Matt E. Jastram	Affirmative	
5	PPL Generation LLC	Annette M Bannon	Affirmative	
5	PSEG Fossil LLC	Tim Kucey	Affirmative	
5	Public Utility District No. 1 of Chelan County	John Yale	Affirmative	
5	Public Utility District No. 1 of Douglas County	Curtis A Wilkins		
5	Public Utility District No. 1 of Lewis County	Steven Grega		
5	Public Utility District No. 2 of Grant County, Washington	Michiko Sell	Affirmative	
5	Puget Sound Energy, Inc.	Lynda Kupfer	Affirmative	
5	Sacramento Municipal Utility District	Susan Gill-Zobitz	Affirmative	
5	Salt River Project	William Alkema	Affirmative	
5	Santee Cooper	Lewis P Pierce	Affirmative	
5	Seattle City Light	Michael J. Haynes	Affirmative	
5	Seminole Electric Cooperative, Inc.	Brenda K. Atkins		
5	Snohomish County PUD No. 1	Sam Nietfeld	Affirmative	
5	South Carolina Electric & Gas Co.	Edward Magic	Affirmative	
5	South Feather Power Project	Kathryn Zancanella		
5	Southern California Edison Company	Denise Yaffe	Affirmative	
5	Southern Company Generation	William D Shultz	Affirmative	
5	Southern Illinois Power Coop.	Alvis D Lanton		
5	Southern Indiana Gas and Electric Co.	Rob Collins	Affirmative	
5	Tacoma Power	Chris Mattson	Affirmative	
5	Tampa Electric Co.	RJames Rocha	Affirmative	
5	Tenaska, Inc.	Scott M. Helyer	Affirmative	

5	Tennessee Valley Authority	David Thompson	Negative	
5	Tri-State Generation & Transmission Association, Inc.	Mark Stein	Negative	COMMENT RECEIVED
5	U.S. Army Corps of Engineers	Melissa Kurtz	Affirmative	
5	USDI Bureau of Reclamation	Erika Doot	Affirmative	
5	Vandolah Power Company L.L.C.	Douglas A. Jensen		
5	Westar Energy	Bryan Taggart	Affirmative	
5	Wisconsin Electric Power Co.	Linda Horn	Affirmative	
5	Wisconsin Public Service Corp.	Scott E Johnson	Affirmative	
5	Xcel Energy, Inc.	Mark A Castagneri	Affirmative	
6	AEP Marketing	Edward P. Cox	Affirmative	
6	Ameren Missouri	Robert Quinlivan	Affirmative	
6	APS	Randy A. Young	Affirmative	
6	Associated Electric Cooperative, Inc.	Brian Ackermann	Affirmative	
6	Bonneville Power Administration	Brenda S. Anderson	Affirmative	
6	City of Austin dba Austin Energy	Lisa Martin	Affirmative	
6	City of Redding	Marvin Briggs	Affirmative	
6	Cleco Power LLC	Robert Hirchak	Affirmative	
6	Colorado Springs Utilities	Shannon Fair	Affirmative	
6	Con Edison Company of New York	David Balban	Affirmative	
6	Constellation Energy Commodities Group	David J Carlson	Affirmative	
6	Dominion Resources, Inc.	Louis S. Slade	Affirmative	
6	Duke Energy	Greg Cecil	Affirmative	
6	El Paso Electric Company	Luis Rodriguez	Affirmative	
6	FirstEnergy Solutions	Kevin Querry	Affirmative	
6	Florida Municipal Power Agency	Richard L. Montgomery	Affirmative	
6	Florida Power & Light Co.	Silvia P Mitchell	Affirmative	
6	Great River Energy	Donna Stephenson	Affirmative	
6	Kansas City Power & Light Co.	Jessica L Klinghoffer	Affirmative	
6	Lakeland Electric	Paul Shipps	Affirmative	
6	Lincoln Electric System	Eric Ruskamp	Affirmative	
6	Los Angeles Department of Water & Power	Brad Packer	Affirmative	
6	Lower Colorado River Authority	Michael Shaw	Affirmative	
6	Luminant Energy	Brenda Hampton	Affirmative	
6	Manitoba Hydro	Blair Mukanik	Affirmative	
6	Modesto Irrigation District	James McFall	Affirmative	
6	Muscatine Power & Water	John Stolley		
6	New York Power Authority	Saul Rojas	Affirmative	
6	North Carolina Municipal Power Agency #1	Matthew Schull	Affirmative	
6	Northern California Power Agency	Steve C Hill	Affirmative	
6	Northern Indiana Public Service Co.	Joseph O'Brien	Affirmative	
6	NRG Energy, Inc.	Alan Johnson	Affirmative	
6	Oglethorpe Power Corporation	Donna Johnson	Affirmative	
6	Oklahoma Gas and Electric Co.	Jerry Nottnagel	Affirmative	
6	Omaha Public Power District	Douglas Collins	Affirmative	
6	PacifiCorp	Sandra L Shaffer	Affirmative	
6	Platte River Power Authority	Carol Ballantine	Affirmative	
6	Portland General Electric Co.	Shawn P Davis	Affirmative	
6	Power Generation Services, Inc.	Stephen C Knapp	Affirmative	
6	Powerex Corp.	Gordon Dobson-Mack	Abstain	
6	PPL EnergyPlus LLC	Elizabeth Davis	Affirmative	
6	PSEG Energy Resources & Trade LLC	Peter Dolan	Affirmative	
6	Public Utility District No. 1 of Chelan County	Hugh A. Owen	Affirmative	
6	Sacramento Municipal Utility District	Diane Enderby	Affirmative	
6	Salt River Project	William Abraham	Affirmative	
6	Santee Cooper	Michael Brown	Affirmative	
6	Seattle City Light	Dennis Sismaet	Negative	
6	Seminole Electric Cooperative, Inc.	Trudy S. Novak	Affirmative	
6	Snohomish County PUD No. 1	Kenn Backholm	Affirmative	
6	South Carolina Electric & Gas Co.	Matt H Bullard	Affirmative	
6	Southern California Edison Company	Joseph T Marone	Affirmative	
6	Southern Company Generation and Energy Marketing	John J. Ciza	Affirmative	
6	Southern Indiana Gas and Electric Co.	Brad Lisembee	Affirmative	
6	Tacoma Public Utilities	Michael C Hill	Affirmative	
6	Tampa Electric Co.	Benjamin F Smith II	Affirmative	
6	Tennessee Valley Authority	Marjorie S. Parsons	Negative	

6	Westar Energy	Grant L Wilkerson		
6	Western Area Power Administration - UGP Marketing	Peter H Kinney	Affirmative	
6	Wisconsin Public Service Corp.	David Hathaway	Affirmative	
6	Xcel Energy, Inc.	Peter Colussy	Affirmative	
7	Eastman Chemical Company	David L Moore		
7	Occidental Chemical	Venona Greaff	Affirmative	
7	Praxair Inc.	David Meade		
7	Siemens Energy, Inc.	Frank R. McElvain	Affirmative	
7	Valero Services, Inc.	Lee W Morris	Affirmative	
8		Roger C Zaklukiewicz	Affirmative	
8		Debra R Warner	Negative	COMMENT RECEIVED
8		David L Kiguel	Negative	
8	Foundation for Resilient Societies	William R Harris	Negative	
8	Massachusetts Attorney General	Frederick R Plett	Affirmative	
8	Volkmann Consulting, Inc.	Terry Volkmann	Negative	
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson	Abstain	
9	Idaho State Public Utilities Commission	Johanna Bell	Affirmative	
9	National Association of Regulatory Utility Commissioners	Jerry M Maio	Abstain	
10	Florida Reliability Coordinating Council	Linda Campbell	Affirmative	
10	Midwest Reliability Organization	Russel Mountjoy	Affirmative	
10	New York State Reliability Council	Alan Adamson		
10	Northeast Power Coordinating Council	Guy V. Zito	Abstain	
10	ReliabilityFirst Corporation	Anthony E Jablonski	Affirmative	
10	SERC Reliability Corporation	Joseph W Spencer	Negative	
10	Southwest Power Pool RE	Bob Reynolds	Negative	
10	Texas Reliability Entity, Inc.	Derrick Davis	Abstain	
10	Western Electricity Coordinating Council	Steven L. Rueckert	Affirmative	

Legal and Privacy : 404.446.2560 voice : 404.467.0474 fax : 3353 Peachtree Road, N.E. : Suite 600, North Tower : Atlanta, GA 30326
Washington Office: 1325 G Street, N.W. : Suite 600 : Washington, DC 20005-3801

Account Log-In/Register

Exhibit G

Standard Drafting Team Roster

Project 2014-04 Physical Security

Standard Drafting Team

Name and Title	Company and Address	Contact Info	Bio
Susan Ivey Chair	2301 Market St. Philadelphia, PA 19103	215-841-4706 SusanO'Brien.Ivey@exeloncorp.com	Ms. Ivey is Vice President of the Transmission Strategy & Compliance of Exelon. She is responsible for oversight of the electric transmission systems of the Exelon Utilities of BGE, ComEd and PECO located in Baltimore, Chicago and Philadelphia, respectively. Ms. Ivey coordinates the efforts for electric transmission operations and long-term planning for all three companies, and manages the interface with regulatory authorities and all transmission interconnected third parties. Ms. Ivey oversees and administers the NERC Compliance Program for Exelon. She also leads the coordination of physical security practices across the Exelon Utilities to ensure alignment of strategies and programs for addressing security risks associated with the electric and gas businesses.
Lou Oberski Vice-Chair	Dominion Resources Services, Inc. 120 Tredegar St Richmond, VA 23219	804-819-2837 Lou.Oberski@dom.com	Mr. Oberski is Managing Director of the Regulation and NERC Compliance Policy for Dominion Resources Services, Inc. He is responsible for administration of all aspects of Dominion's corporate NERC compliance assurance programs and oversees Dominion's involvement at NERC and its sub-regions as well as FERC and RTO policy coordination for Dominion at PJM, ISO-New England and the MidContinent ISO. Prior to Mr. Oberski's current position, his career at Dominion covered increasing management responsibilities in transmission engineering, operations, planning and maintenance. The most recent 10 years have focused on developing, establishing and coordinating NERC and RTO policy at Dominion with a particular emphasis on generation supplier policy at NERC and RTOs. Mr. Oberski is a member of the North American Energy Standards Board, Board of Directors and past chair of its Executive Committee. He is also a member of EEI's Reliability Executive Advisory Committee, the SERC Board of Directors and SERC Board Executive Committee. Mr. Oberski has been employed by Dominion for 30 years and holds a Bachelor's degree in electrical engineering from Western Michigan University.
John Breckenridge	KCP&L 1200 Main Street 18th Floor KCMO 64106	816-654-1725 john.breckenridge@kcpl.com	Mr. Breckenridge is the Senior Manager of Corporate Security for Kansas City Power & Light based in Kansas City, MO. In his current capacity, Mr. Breckenridge directs the overall Corporate Security function to ensure security operations are in compliance with legal, regulatory, and company requirements. Corporate Security responsibilities

			include physical security, investigations, guard force management, protection operations, law enforcement liaison, enterprise-wide crisis management and business continuity planning. To be effective, Mr. Breckenridge uses his 25 plus years of military, criminal justice and industrial security experience to work with each functional department and business unit. Mr. Breckenridge began his career while in the U.S. Army, where he was instrumental in supporting many special security operations throughout the U.S. and in many countries, especially during his assignment in Europe. In addition to his eight-year career in the military, Mr. Breckenridge worked for six years in the Jackson County, MO. criminal justice system. During this time, Mr. Breckenridge specialized in security systems, close protection operations and special event security functions first with the Department of Corrections and then in conjunction with the Jackson County Courts. From 1993 until 2008, Mr. Breckenridge was the Director of Security and Chief Security Officer for Aquila Energy until Aquila was purchased by Kansas City Power & Light. Mr. Breckenridge is Board Certified in Security Management as a Certified Protection Professional, holds a BLA degree and a degree with an emphasis in Criminal Justice, and is a Licensed Private Investigator and an active member of several security related professional organizations. Mr. Breckenridge has been featured as a Guest Lecturer for successful business approaches to security issues and has also been featured in several trade and regional publications.
Ross Johnson	Capital Power	(780) 405-5542 rjohnson@capitalpower.com	Mr. Johnson, CPP is the Senior Manager of Security and Contingency Planning for Capital Power. He served in the Canadian Forces as an infantry and intelligence officer for 24 years. Since leaving the service in 2001, Mr. Johnson has been employed in several security-related leadership positions in aviation security, the offshore oil industry, and the electricity sector. Prior to joining Capital Power in 2009, Mr. Johnson was the Director of Security and Contingency Planning with EPCOR Utilities. Mr. Johnson is the author of Antiterrorism Planning and Threat Response, a book on the prevention of terrorist attacks. Mr. Johnson is a member of the NERC Critical Infrastructure Protection Committee, where he sits on the Executive Committee. He is also Chair of the Committee's Physical Security Working Group, and the leader of the Physical Security Roundtable Group. Mr. Johnson is Chair of the Canadian Electricity Association's Security and Infrastructure Protection Committee, and Chair of ASIS

			International's Petrochemical, Chemical, and Extractive Industries Security Council. Mr. Johnson has a Baccalaureate in Military Arts and Sciences with Distinction, and is board-certified in security management by ASIS International.
Kathleen Judge	National Grid 939 Southbridge Street, Worcester, MA 01610	(508) 860-6040 Kathleen.judge@nationalgrid.com	Ms. Judge is Director of Risk and Compliance for Security at National Grid, where she has worked for 25+ years. She is responsible for managing National Grid's strategies and best practices required to protect energy delivery facilities in accordance with governing security regulations in the US. As part of this Ms. Judge is actively engaged with state and federal regulatory authorities to shape policies and procedures. For example, at the federal level she works with the Infrastructure Security Compliance Division of DHS, the United States Coast Guard and the Pipeline Security Division of the Transportation Security Administration. Ms. Judge was also the chair of the American Gas Association Security Committee and currently serves as an AGA representative on the Oil & Natural Gas Sector Coordinating Council. She is also actively involved in the EEI Security Committee and serves on the Executive Steering Committee for the Long Island Sound Area Maritime Security Committee. In prior roles, she was responsible for, and a key member on, delivering Company's business plan for a deregulated energy market, serving as the strategic and operational expert on electricity restructuring for Massachusetts, Rhode Island, New Hampshire and New York. She was also an active member of the North American Energy Standards Board Retail Electric Quadrant, developing model business practices for deregulated marketplaces. Leading up to this, Ms. Judge was a key developer and implementer of an award winning renewable energy program in Massachusetts and Rhode Island. Ms. Judge holds a Masters of Business Administration degree from Nichols College.
Mike O'Neil	Florida Power & Light 700 Universe Blvd., Juno Beach, Fl. 33408	(561) 904-3503 mco0hwz@fpl.com	Mr. O'Neil is Director of the Power Delivery Compliance & Regulatory. He is responsible for business unit execution compliance to transmission based FERC requirements for FPL and NERC transmission reliability standards for FPL and NEER facilities throughout the country.
Stephen Pelcher	Santee Cooper One Riverwood Drive Moncks Corner, SC 29461	843-761-4016 srpelche@santeecooper.com	Mr. Pelcher is Deputy General Counsel Nuclear and Regulatory Compliance at Santee Cooper. Mr. Pelcher joined Santee Cooper in 1996. Prior to working for Santee Cooper, he was Senior Attorney for Duquesne Light Company in Pittsburgh (1990 to 1996). Mr. Pelcher has been a practicing attorney

			for more than 31 years and has worked in the electric utility industry for 24 years. Among other duties, Mr. Pelcher is the lead Santee Cooper company attorney in all matters within the jurisdiction of the FERC under Part II of the Federal Power Act; the lead company attorney relating to interpretation of requirements embedded within standards established by NERC under Section 215 of the Federal Power Act and current Chair of Santee Cooper's internal Reliability Standards Compliance Coordination Committee. Mr. Pelcher has a Bachelor of Arts degree in Philosophy from the University of Pittsburgh, College of Arts and Sciences; a Juris Doctor from the University of Pittsburgh, School of Law; and an LL.M (Taxation) from the Dickinson School of Law, Pennsylvania State University.
John Pespisa	Southern California Edison 2244 Walnut Grove Ave. Rosemead, Ca 91770	626-688-6291 John.pespisa@sce.com	Mr. Pespisa is Director of SCE's NERC Compliance program and Acting Director of SCE's Security Technology & Compliance group. Mr. Pespisa started his career with Southern California Edison in 1987, starting in transmission operations and electrical substations. Since then he has worked in positions of increasing responsibility including operation of SCE's bulk electric and distribution systems, and supervisory positions at SCE's Energy Control Center, including Manager of short term power marketing, and Manager of Real-Time Power Operations. In 2011, he moved to his current position as the Director of SCE's NERC Compliance Program In his current role he oversees SCE's compliance with federal Reliability Standards, which have been promulgated to ensure the safe, reliable operation of the power grid, and to protect the grid's critical infrastructure against cyber threats. Mr. Pespisa is a graduate of California State Los Angeles and hold degrees in Electrical Engineering and Business Management.
Robert Rhodes	Southwest Power Pool 201 Worthen Drive Little Rock, AR 72223	501-614-3241 rrhodes@spp.org	Mr. Rhodes is the Manager of Reliability Standards at Southwest Power Pool (SPP) where he has been employed since 2000. In his previous role at SPP he was Manager of Reliability Coordination for over 10 years. Prior to joining SPP, Mr. Rhodes worked at Progress Energy (Carolina Power & Light Company) in Raleigh, NC for over 26 years in various positions in transmission maintenance, operations and planning. In his current capacity, Mr. Rhodes works with SPP members, SPP staff and other industry experts to ensure that reliability standards necessary to maintain a reliable bulk electric system are in place. He coordinates SPP members and registered entities in the development, refinement, maintenance, communication, training and implementation of national and regional reliability standards and policies.

			Mr. Rhodes is active at NERC currently serving on the Operating Reliability Subcommittee (ORS), the ORS Executive Committee, the Resources Subcommittee, the Standards Committee Process Subcommittee, the Reliability Coordination Standard Drafting Team, the Operating Personnel Communications Protocols Standard Drafting Team and the TOP/IRO Revisions Standard Drafting Team. He has previously served on the Reliability Coordinator Working Group, the Interchange Distribution Calculator Working Group and was Vice Chair of the Distribution Factor Working Group. Additionally, he has served on committees, working groups and task forces in SPP, SERC and VACAR. Mr. Rhodes received an Associate in Science degree from Rockingham Community College in 1970, a Bachelor of Science degree in Electrical Engineering from North Carolina State University in 1972 and a Master of Engineering degree from Rensselaer Polytechnic Institute in 1974. He is a member of Tau Beta Pi, Eta Kappa Nu, Order of the Engineer, the Institute of Electrical and Electronics Engineers and its Power Engineering Society and the National Society of Professional Engineers. He is a NERC Certified System Operator (Reliability) and is a registered professional engineer in the State of North Carolina.
Allan Wick	Tri-State Generation & Transmission Association, Inc. 1100 W. 116th Ave., Westminster, CO 80234	303-254-3341 awick@tristategt.org	Mr. Wick is a 30 year security executive, 13 in the energy sector with a comprehensive industry perspective after working for an investor owned utility, independent system operator and now at a cooperative generation and transmission company - where he serves as their Enterprise Security Manager & Chief Security Officer. He is a member of the ASIS International Utilities Security Council and the WECC Physical Security Working Group since 2005. He also served for six years on the ASIS International Certification Board of Directors. Mr. Wick has designed and implemented enterprise-wide physical security programs for three different organizations, served as a drafting team member for five ANSI standards, and has authored a number of security related magazine articles and white papers. Mr. Wick received his MBA from Webster University and holds multiple security and business continuity certifications, including CPP, PSP, CBCP, CFE, and PCI.
Manho Yeung	Pacific Gas and Electric Company Mail Code N9G, P.O. Box 770000 San Francisco, California, 94177	415-973-7649 MxY6@pge.com	Mr. Yeung is Senior Director of System Planning and Reliability, for Pacific Gas and Electric Company and is responsible for electric transmission and distribution planning, asset and risk management and reliability improvements. Mr. Yeung oversees PG&E's capital investment plan in expanding, upgrading and modernizing its 18,500

			miles of electric transmission lines, 850 substations, and 140,000 miles of distribution lines. Mr. Yeung has been with Pacific Gas and Electric Company since 1980 and has over 30 years of energy policy, electric generation planning, electric T&D planning, asset and risk management, project management, engineering, and operations experience. Mr. Yeung received his Bachelor of Science degree in electric engineering from the Georgia Institute of Technology, and a Master of Science degree in electric engineering from the Santa Clara University. Manho is a registered professional electric engineer in the State of California.
Stephen Crutchfield Standards Developer	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	609-651-9455 Stephen.crutchfield@nerc.net	Mr. Crutchfield is the lead NERC Staff Coordinator for Project 2014-04, Physical Security. Stephen began his career with NERC in May 2007. Prior to joining NERC, Mr. Crutchfield was a Project Manager with Shaw Energy Delivery Services, managing engineering and construction projects in the substation and transmission line fields. Mr. Crutchfield's background also includes experience with PJM as Manager of RTO Integration, working on the operations and markets integration of new members (AEP, ComEd, Dayton, Dominion and Duquesne) into PJM and southern seams operations issues with Progress Energy, Duke and TVA. Stephen also helped lead the team that was developing GridSouth in the dual roles of Organization Architect and Manager of Customer Support. Prior to GridSouth, Mr. Crutchfield was the Manager of Power System Operations Training at Progress Energy where he spent over 10 years training System Operators and Engineers. Overall, Stephen was with Progress Energy for 16 years. Mr. Crutchfield received his Bachelor of Arts in Physics from the University of Virginia and Masters of Science in Electrical Engineering from North Carolina State University. Stephen holds a Master of Science in Management degree, also from North Carolina State University. Mr. Crutchfield is also a member of the Institute of Electrical and Electronic Engineers and the Power and Energy Society.
Steven Noess Associate Director of Standards Development, Standards	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	404-217-9691 steven.noess@nerc.net	Mr. Noess is Associate Director of Standards Development at the North American Electric Reliability Corporation (NERC) in Atlanta, GA, and has been employed by NERC since 2011. Prior to joining NERC, Mr. Noess was an attorney at the Minnesota Legislature. Before becoming an attorney, Mr. Noess was an officer in the United States Army. Mr. Noess has a bachelor's of science degree from the U.S. Military Academy, West Point, NY, and a law degree from the University of Minnesota Law School.

Mark Olson Standards Developer	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	404-446-9760 Mark.olson@nerc.net	Mr. Olson is a Standards Developer at the North American Electric Reliability Corporation (NERC), and has been employed by NERC since 2012. Previously he was a career officer in the U.S. Navy where he served in various positions related to the operations and management of surface ships and naval personnel. Mr. Olson has a master's degree in electrical engineering from the Naval Postgraduate School and a bachelor's degree from the U.S. Naval Academy.
Brian Harrell Director, ES-ISAC Operations	Electricity Sector Information Sharing and Analysis Center North American Electric Reliability Corporation 1325 G Street NW, Suite 600 Washington, DC 20005	202-400-3003 office | 609-651-0671 (c) Brian.Harrell@nerc.net	Mr. Harrell is the Director, ES-ISAC Operations for the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) at the North American Electric Reliability Corporation (NERC), joining NERC in August 2010. In this capacity he is responsible for managing situational awareness, incident management, and security coordination for the electricity sector through timely, reliable and secure information exchange. Mr. Harrell has 18 years of experience in the security industry serving in organizations such as law enforcement, military, and corporate security, among others. Mr. Harrell is formerly the NERC Director of Critical Infrastructure Protection Programs, as well as the CIP Manager for the SERC Reliability Corporation, where he oversaw electricity security related matters. Prior to joining SERC, Mr. Harrell was the Sector Security Specialist for the Infrastructure Security Compliance Division at the U.S. Department of Homeland Security (DHS). Brian specialized in securing high risk facilities and Continuity of Operations (COOP) for DHS. Mr. Harrell also served in the US Marine Corps as an Anti-Terrorism and Force Protection Instructor.
Bob Canada Manager, Outreach & Training	North American Electric Reliability Corporation 3353 Peachtree Road, NE, Suite 600 - North Tower Atlanta, GA 30326	404-446-9709 bob.canada@nerc.net	Mr. Canada presently serves as the Manager, Outreach and Training, at the NERC and is the staff support and Secretary to the Critical Infrastructure Protection Committee standing committee. Mr. Canada was previously employed in the electric industry for 32 years with Southern Company in various roles with corporate security and was Manager of Corporate Security at Georgia Power Company from March 1995 - December 2002. Responsibilities included corporate and internal investigations, physical security of employees and corporate assets. Mr. Canada directed alarm systems design and installation as well and was responsible for the overall corporate response for security at Georgia Power Co. He also directed the Georgia Power and Southern Company Security Planning for the Atlanta Olympic Games. Responsible for the development of the corporate security plan along with the

			implementation and daily operations included physical security of the transmission and distribution facilities supporting the Olympic venues, monitoring the protective countermeasures in place, consulting with Federal, State and Local Law Enforcement Agencies to protect the State, Metropolitan and Atlanta Electrical Infrastructure. Mr. Canada served two terms for the Southeastern Reliability Council (SERC) as the first Chairman of the Critical Infrastructure Protection Committee and represented SERC on the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Committee (CIPC) as the Physical Security voting member. Subsequently, he was elected by the CIPC as a Vice Chair for four terms. Mr. Canada received his Bachelor's degree from West Georgia State University and also holds a Juris Doctor from the Woodrow Wilson College of Law.