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

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