**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 STANDARDS CIP-013-1, CIP-005-6, AND CIP-010-3 ADDRESSING SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT


Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net

*Counsel for the North American Electric Reliability Corporation*


September 26, 2017

# 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 STANDARDS CIP-013-1, CIP-005-6, AND CIP-010-3 ADDRESSING SUPPLY CHAIN CYBERSECURITY RISK MANAGEMENT

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 Order No. 829,[3] the North American Electric Reliability Corporation ("NERC")[4] hereby submits for Commission approval proposed Reliability Standards CIP-013-1 – Cyber Security – Supply Chain Risk Management, CIP-005-6 – Cyber Security – Electronic Security Perimeter(s), and CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments. The proposed Reliability Standards address the Commission's directives from Order No. 829 to develop new or modified Reliability Standards that address supply chain cybersecurity risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System ("BES") operations.[5] NERC requests that the

[1] 16 U.S.C. § 824o (2012).

[2] 18 C.F.R. § 39.5 (2017).

[3] Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards*, 156 FERC ¶ 61,050 (2016) ("Order No. 829").

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

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

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

NERC also requests approval of: (1) the associated Implementation Plan (Exhibit B); the associated Violation Risk Factors ("VRFs") and Violation Severity Levels ("VSLs") (Exhibit F); and the retirement of currently-effective Reliability Standards CIP-005-5 and CIP-010-2, which are superseded by proposed Reliability Standards CIP-005-6 and CIP-010-3, respectively.

As required by Section 39.5(a) of the Commission's regulations,[6] this Petition presents the technical basis and purpose of the proposed Reliability Standards, a summary of the development history (Exhibit G), and a demonstration that the proposed Reliability Standards meet the criteria identified by the Commission in Order No. 672[7] (Exhibit C). The NERC Board of Trustees ("Board") adopted the proposed Reliability Standards on August 10, 2017.

## I. EXECUTIVE SUMMARY

The proposed Reliability Standards are designed to augment NERC's cybersecurity Critical Infrastructure Protection ("CIP") Reliability Standards to further mitigate cybersecurity risks associated with the supply chain for BES Cyber Systems, consistent with Order No. 829. In that order, the Commission found that supply chains for information and communications technology and industrial control systems present risks to BES security, providing various opportunities for adversaries to initiate cyberattacks.[8] The Commission stated that "[t]he targeting of vendors and software applications with potentially broad access to BES Cyber Systems marks

---

6 18 C.F.R. § 39.5(a).

7 Order No. 672, *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, FERC Stats. & Regs. ¶ 31,204, 114 FERC 61,104 at PP 262, 321-37, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212, 114 FERC 61,328 (2006).

8 Order No. 829 at PP 25-34. For example, supply chain risks include the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices.

a turning point in that it is no longer sufficient to focus protection strategies exclusively on post-acquisition activities at individual entities."[9] The Commission thus directed NERC "to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations."[10]

The proposed Reliability Standards address the Commission's directive in Order No. 829 and enhance the cybersecurity posture of the electric industry by requiring Responsible Entities[11] to take additional actions to address cybersecurity risks associated with the supply chain for BES Cyber Systems.[12] Consistent with Order No. 829, the proposed Reliability Standards focus on the following four security objectives: (1) software integrity and authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls. Collectively, the requirements in the proposed Reliability Standards are designed to:

- Reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System.
- Address vendor remote access-related threats, including the threat that vendor credentials could be stolen and used to access a BES Cyber System without the Responsible Entity's knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a Responsible Entity's BES Cyber System.
- Address the risk that Responsible Entities could unintentionally plan to procure and install unsecure equipment or software within their information systems, or could unintentionally

---

9 *Id*. at P 34 (internal citations omitted).

10 *Id*. at P 2 (internal citations omitted).

11 As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entities subject to the CIP Reliability Standards.

12 The CIP Reliability Standards currently include a number of requirements that help mitigate supply chain risks. *See Comments of the North American Electric Reliability Corporation In Response to Notice of Proposed Rulemaking*, at 15-16, Docket No. RM15-14-000 (Sept. 21, 2015).

fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions.

- Address the risk that Responsible Entities could enter into contracts with vendors who pose significant risks to their information systems, as well as the risk that products procured by a Responsible Entity fail to meet minimum security criteria.

- Address the risk that a compromised vendor would not provide adequate notice of security events and vulnerabilities, and related incident response to Responsible Entities with whom that vendor is connected.

Specifically, proposed new Reliability Standard CIP-013-1 requires Responsible Entities to develop and implement plans to address supply chain cybersecurity risks during the planning and procurement of high and medium impact BES Cyber Systems. As discussed in greater detail below, proposed Reliability Standard CIP-013-1 improves reliability by requiring Responsible Entities to implement processes to: (1) identify and assess cybersecurity risks to the BES from vendor products and services in their planning activities for high and medium impact BES Cyber Systems; and (2) include specified security concepts in their procurement activities for high and medium impact BES Cyber Systems.

Additionally, the proposed modifications in CIP-005-6 and CIP-010-3 bolster the protections in the currently-effective CIP Reliability Standards by addressing specific risks related to vendor remote access and software integrity and authenticity, respectively, in the operational phase of the system life cycle. Pursuant to Requirement R2, Parts 2.4 and 2.5 of proposed Reliability Standard CIP-005-6, Responsible Entities must have one or more methods for: (1) determining active vendor remote access sessions (Part 2.4); and (2) disabling active vendor remote access (Part 2.5). The security objective of these requirement parts is to control vendor remote access to mitigate risks associated with unauthorized access.

Further, pursuant to Requirement R1, Part 1.6 of proposed Reliability Standard CIP-010-3, prior to installing software, Responsible Entities must verify the identity of the software source

and the integrity of the software obtained by the software sources, when methods are available to do so. The security objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit.

The proposed Reliability Standards would add to the defense-in-depth approach of the CIP Reliability Standards by strengthening the required protections that help mitigate supply chain risks. For the reasons discussed herein, NERC respectfully requests that the Commission approve the proposed Reliability Standards as just, reasonable, not unduly discriminatory, or preferential, and in the public interest.

Supply chain management, however, is a complex global issue. Supply chains for information and communications technology and industrial control systems are long and multidimensional, involving numerous parties in a multitude of countries across the globe. Registered entities typically rely on a number of vendors and contractors that may use multiple third-party suppliers for components used in their products or technologies. Multiple entities across the globe may participate in the development, design, manufacturing, and delivery of a single product purchased by a registered entity. As mandatory Reliability Standards under Section 215 of the FPA have limited applicability – they cannot directly impose obligations on suppliers, vendors, or other entities that provide products or services to registered entities[13] – NERC Reliability Standards should not be expected to mitigate all risks inherent to the global supply chain.

[13] As the Commission stated in Order No. 829 (at P 21), "any action taken by NERC in response to the Commission's directive to address the supply chain-related reliability gap should respect 'section 215 jurisdiction by only addressing the obligations of responsible entities' and 'not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities.'"

In conjunction with the adoption of the proposed Reliability Standards, the Board issued a series of resolutions directing NERC to continue working with industry and vendors on supply chain issues, including preparation for implementing the proposed Reliability Standards, further studying of supply chain risks, and continued information sharing, among other activities, as further discussed below.[14] To that end, NERC is committed to using its many reliability tools – e.g., guidelines, training exercises, alerts, information sharing and analysis – to support industry's efforts to mitigate supply chain risks and engage vendors to identify and address emerging supply-chain risks.

## II. NOTICES AND COMMUNICATIONS

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


Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W.
Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net

Howard Gugel
Senior Director, Standards and Education
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
howard.gugel@nerc.net


## III. BACKGROUND

### A. Regulatory Framework

By enacting the Energy Policy Act of 2005,[15] Congress entrusted the Commission with the duties of approving and enforcing rules to ensure the reliability of the Bulk-Power System, and with the duty of certifying an ERO that would be charged with developing and enforcing

[14] The Board's resolutions are available at http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

[15] 16 U.S.C. § 824o.

mandatory Reliability Standards, subject to Commission approval. Section 215(b)(1) 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.[16] Section 215(d)(5) of the FPA authorizes the Commission to order the ERO to submit a new or modified Reliability Standard.[17] Section 39.5(a) 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.[18]

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 and Section 39.5(c) 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.[19]

### B. NERC Reliability Standards Development Procedure

The proposed Reliability Standards were developed in an open and fair manner and in accordance with the Commission-approved Reliability Standard development process.[20] NERC develops Reliability Standards in accordance with Section 300 (Reliability Standards

16 *Id.* § 824(b)(1).

17 *Id.* § 824o(d)(5).

18 18 C.F.R. § 39.5(a).

19 16 U.S.C. § 824o(d)(2); 18 C.F.R. § 39.5(c)(1).

20 Order No. 672 at P 334.

Development) of its Rules of Procedure and the NERC Standard Processes Manual.[21] 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 criteria for approving Reliability Standards.[22] 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. Further, a vote of stakeholders and adoption by the Board is required before NERC submits the Reliability Standard to the Commission for approval.

### C. Order No. 829 Directives

As noted above, in Order No. 829, the Commission directed NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations. The Commission stated that the new or modified Reliability Standard is intended to mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System.[23] The Commission further specified:

> [W]e direct NERC to develop a forward-looking, objective-based Reliability Standard to require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. The new or modified Reliability Standard should address the following security objectives…: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. In making this directive, the Commission does not require NERC to impose any specific controls, nor does the Commission require NERC to propose "one-size-fits-all" requirements. The new or modified Reliability Standard

---

[21] 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.

[22] ERO Certification Order at P 250.

[23] Order No. 829 at P 1.

> should instead require responsible entities to develop a plan to meet the four objectives, or some equally efficient and effective means to meet these objectives, while providing flexibility to responsible entities as to how to meet those objectives.[24]

For the first objective, software integrity and authenticity, the Commission specified that the "new or modified Reliability Standard must address verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and (2) the integrity of the software and patches before they are installed in the BES Cyber System environment."[25] The Commission stated that "[t]his objective is intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System."[26]

For the second objective, vendor remote access, the Commission specified that the "new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions," for both user-initiated and machine-to-machine vendor remote access.[27] The Commission explained that "this objective addresses the threat that vendor credentials could be stolen and used to access a BES Cyber System without the responsible entity's knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a responsible entity's BES Cyber System."[28] Further, the Commission stated that the "controls adopted under this objective should give

---

24 *Id*. at P 2.

25 *Id*. at P 48.

26 *Id*. at P 49.

27 *Id*. at P 51.

28 *Id*. at P 52.

responsible entities the ability to rapidly disable remote access sessions in the event of a system breach."[29]

For the third objective, information system planning, the Commission specified that the "new or modified Reliability Standard must address how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes," including "a responsible entity's CIP Senior Manager's (or delegate's) identification and documentation of the risks of proposed information system planning and system development actions."[30] The Commission explained that this "objective is intended to ensure adequate consideration of these risks, as well as the available options for hardening the responsible entity's information system and minimizing the attack surface."[31] This objective "addresses the risk that responsible entities could unintentionally plan to procure and install unsecure equipment or software within their information systems, or could unintentionally fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions."[32]

For the fourth objective, vendor risk management and procurement controls, the Commission specified that the "new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."[33] The Commission further stated that NERC must address the following topics for this objective: (1) vendor security event notification processes; (2) vendor personnel termination

---

29 *Id*.

30 *Id*. at P 56.

31 *Id*.

32 *Id*. at P 57.

33 *Id*. at P 59.

notification for employees with access to remote and onsite systems; (3) product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (4) coordinated incident response activities; and (5) other related aspects of procurement.[34] The Commission explained that this objective "addresses the risk that responsible entities could enter into contracts with vendors who pose significant risks to their information systems, as well as the risk that products procured by a responsible entity fail to meet minimum security criteria" and "the risk that a compromised vendor would not provide adequate notice and related incident response to responsible entities with whom that vendor is connected."[35]

In addition, FERC specified that the new or modified Reliability Standard should include "a periodic reassessment of the utility's selected controls," by requiring the Responsible Entity's CIP Senior Manager to review and approve the controls adopted to meet the specific security objectives identified in the Reliability Standard at least every 15 months.[36] The Commission explained that this periodic assessment "should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities."[37]

### D. Development of the Proposed Reliability Standards

As further described in Exhibit G hereto, following the issuance of Order No. 829, NERC initiated a Reliability Standard development project, Project 2016-03 Cyber Security Supply Chain Risks Management ("Project 2016-03"), to address the directives from Order No. 829. On January 19, 2017, NERC posted the initial draft of proposed Reliability Standard CIP-013-1 for a 45-day comment period and ballot. The initial ballot did not receive the requisite approval from the

---

34 *Id*.

35 *Id*. at P 60.

36 *Id*. at P 46.

37 *Id*.

registered ballot body ("RBB"). After considering comments to the initial draft, NERC posted a second draft of CIP-013-1 for another 45-day comment period and ballot on May 2, 2017. Concurrently, NERC posted initial drafts of CIP-005-6 and CIP-010-3 for a 45-day comment period and ballot. The subject of the modifications in CIP-005-6 and CIP-010-3 were included in the initial draft of CIP-013-1. The second draft of CIP-013-1 received the requisite approval from the RBB with an affirmative vote of 88.64%. The initial drafts of CIP-005-6 and CIP-010-3 also received the requisite approval from the RBB with an affirmative votes of 89.84 % and 82.92%, respectively. NERC conducted 10-day final ballots for these proposed Reliability Standards, which received affirmative votes of 84.19% for CIP-013-1, 88.79% for CIP-005-6, and 81.4% for CIP-010-3. The Board adopted the proposed Reliability Standards on August 10, 2017.

## IV. JUSTIFICATION FOR APPROVAL

As discussed below and in Exhibit C, the proposed Reliability Standards address the Commission's directives in Order No. 829 and are just, reasonable, not unduly discriminatory, or preferential, and in the public interest. The following section provides an explanation of:

- the purpose of the proposed Reliability Standards (Subsection A);
- the scope and applicability of the proposed Reliability Standards (Subsection B);
- the requirements in proposed Reliability Standard CIP-013-1, including a discussion of the manner in which they address the objectives discussed in Order No. 829 (Subsection C);
- the additional requirements in proposed Reliability Standard CIP-005-6, including a discussion of the manner in which they address the objectives discussed in Order No. 829 (Subsection D);
- the additional requirements in proposed Reliability Standard CIP-010-3, including a discussion of the manner in which they address the objectives discussed in Order No. 829 (Subsection E); and
- the enforceability of the proposed Reliability Standards (Subsection G).

### A. Purpose and Overview of the Proposed Reliability Standards

As noted above, the purpose of the proposed Reliability Standards is to enhance the cybersecurity posture of the electric industry by requiring Responsible Entities to take additional actions to address cybersecurity risks associated with the supply chain for BES Cyber Systems. The CIP Reliability Standards currently include a number of requirements that help mitigate supply chain risks.[38] As discussed in Order No. 829, however, security issues associated with potential supply chain disruption or compromise present a significant threat to the BES and increased attention should be focused on minimizing the attack surfaces of information and communications technology products and services procured to support BES operations.[39] To that end, the proposed Reliability Standards are designed to augment the existing controls required in the currently-effective CIP Reliability Standards that help mitigate supply chain risks.

As discussed further below, proposed Reliability Standard CIP-013-1 focuses on the planning and procurement phases of BES Cyber Systems, requiring Responsible Entities to develop and implement plans to address supply chain cybersecurity risks during the planning and procurement of high and medium impact BES Cyber Systems. The security objective of the supply chain cybersecurity risk management plans is to ensure that Responsible Entities consider the security, integrity, quality, and resilience of the supply chain, and take appropriate mitigating action when procuring BES Cyber Systems to address threats and vulnerabilities in the supply chain. As discussed below, the supply chain cybersecurity risk management plans must include processes to: (1) identify and assess cybersecurity risks to the BES from vendor products and services; and (2) include specified security concepts in their procurement activities for high and

---

[38] *See Comments of the North American Electric Reliability Corporation In Response to Notice of Proposed Rulemaking*, at 15-16, Docket No. RM15-14-000 (Sept. 21, 2015).

[39] Order No. 829 at PP 32-34.

medium impact BES Cyber Systems, including (i) vendor security event notification processes, (ii) coordinated incident response activities, (iii) vendor personnel termination notification for employees with access to remote and onsite systems, (iv) vulnerability disclosures, (v) software integrity and authenticity, and (vi) coordination of controls for vendor remote access.

Additionally, the proposed modifications in CIP-005-6 and CIP-010-3 address specific risks related to vendor remote access and software integrity and authenticity that are not already addressed in the currently-effective CIP Reliability Standards. Pursuant to Requirement R2, Parts 2.4 and 2.5 of proposed Reliability Standard CIP-005-6, Responsible Entities must have one or more methods for: (1) determining active vendor remote access sessions (Part 2.4); and (2) disabling active vendor remote access (Part 2.5). Further, pursuant to Requirement R1, Part 1.6 of proposed Reliability Standard CIP-010-3, prior to installing software, Responsible Entities must verify the identity of the software source and the integrity of the software obtained by the software sources, when methods are available to do so.

### B. Applicability and Scope of the Proposed Reliability Standards

#### 1) Applicable Functional Entities and Facilities

Consistent with the Commission's FPA section 215 jurisdiction and Order No. 829,[40] the proposed Reliability Standards apply only to registered entities and do not directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities. While proposed Reliability Standard CIP-013-1 requires applicable registered entities to implement a supply chain risk management plan when they engage with third-party providers of products and services for BES Cyber Systems, it does not directly create any obligations for suppliers, vendors or other entities. The focus is on the steps registered entities take to account for

[40] *Id*. at P 21.

security issues during the planning and procurement phase of high and medium impact BES Cyber Systems. Any resulting obligation that a supplier, vendor or other entity accepts in providing products or services to the registered entity is a contractual matter between the registered entity and the third party outside the scope of the proposed Reliability Standard, as discussed further below. Similarly, the modifications in CIP-005-6 and CIP-010-3 apply solely to registered entities.

The applicability section of the proposed Reliability Standards are the same as those in each of the existing CIP cybersecurity Reliability Standards. The list of functional entities subject to the proposed Reliability Standards is thus the same as those functional entities subject to each of the existing CIP cybersecurity Reliability Standards, CIP-002-5.1a through CIP-011-2.[41] These functional entities include: Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Reliability Coordinators, Transmission Operators, and Transmission Owners. The standard drafting team ("SDT") for Project 2016-03 concluded that the same functional entities subject to the existing CIP cybersecurity Reliability Standards should also be subject to the proposed supply chain cybersecurity risk management requirements as they are intended to accomplish the same purpose: to mitigate the risk of a cybersecurity incident affecting the reliable operation of the BES.

Similarly, the list of Facilities subject to the proposed Reliability Standards is the same as those Facilities included in the existing CIP cybersecurity Reliability Standards. That is, for functional entities other than Distribution Providers, all BES Facilities, systems, and equipment are in scope, unless subject to an exemption listed in Applicability Section 4.2.3. The phrase "BES Facilities, systems, and equipment" refers to the assets that make up or are used to operate the

[41] The only exception is that proposed Reliability Standard CIP-013-1 does not include Interchange Coordinator or Interchange Authority as applicability entities. These functional entities are no longer registered with NERC and subject to NERC Reliability Standards.

BES, such as Transmission stations/substations, generation resources, Protection Systems, and Control Centers. For Distribution Providers, there is a more limited set of Facilities, systems, and equipment subject to the proposed Standards, as provided in Applicability Section 4.2.1. As with the list of functional entities, given that the overall purpose of the proposed Reliability Standards is consistent with the purpose of the existing CIP cybersecurity Reliability Standards, the initial scoping of the Facilities subject to the proposed Reliability Standards should be consistent with the applicability of the existing CIP cybersecurity Reliability Standards.

2) Applicable BES Cyber Systems

As with existing Reliability Standards CIP-004-6 through CIP-011-2, the requirements in the proposed Reliability Standards apply only to BES Cyber Systems designated as medium or high impact pursuant to Reliability Standard CIP-002-5.1a. The currently-effective CIP Reliability Standards apply a risk-based construct, requiring Responsible Entities to identify and categorize BES Cyber Systems as high, medium, or low impact, and then protect those BES Cyber Systems commensurate with the risks they present to the reliable operation of the BES.[42] High and medium impact BES Cyber Systems are associated with those BES Facilities, systems, and equipment that are most critical to interconnected operations. In turn, the CIP Reliability Standards require additional protections for these BES Cyber Systems as compared to those applicable to low impact BES Cyber Systems. The goal of the CIP Reliability Standards is to provide for comprehensive coverage of Cyber Assets that could impact Real-time operations while focusing industry resources on protecting those BES Cyber Systems with heightened risks to the BES. To that end, the Commission recognized in Order No. 791 that the requirements applicable to low impact BES

[42] Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*, 145 FERC ¶ 61,160, 78 Fed. Reg. 72,755 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

Cyber Systems, given their lower risk profile, should not be overly burdensome to divert resources from the protection of medium and high impact BES Cyber Systems.[43]

Reliability Standards CIP-004-6 through CIP-011-3 contain detailed requirements applicable to the protection of high and medium impact, covering the following topics: personnel and training (CIP-004-6);[44] electronic security perimeters and remote access protections (CIP-005-5);[45] physical security (CIP-006-6);[46] systems security management (CIP-007-6);[47] incident reporting and response planning (CIP-008-5);[48] recovery plans (CIP-009-6);[49] configuration change management (CIP-010-2);[50] and BES Cyber System Information protection (CIP-011-2).[51] In contrast, Reliability Standard CIP-003-6 contains all the requirements applicable to low impact BES Cyber Systems, covering the following four subject matter areas: (1) cyber security awareness; (2) physical security controls; (3) electronic access controls; and (4) Cyber Security

---

[43] *Id.* at P 111 (finding that it would be unduly burdensome to require responsible entities to create and maintain an inventory of Low Impact assets for audit purposes).

[44] CIP-004-6 requires Responsible Entities to implement a cyber security awareness program, implement a cyber security training program, conduct background checks for authorizing electronic and unescorted physical access, implement an access management program for authorizing electronic and unescorted physical access, and implement an access revocation program.

[45] CIP-005-5 requires Responsible Entities to manage electronic access by: (1) logically protecting and segmenting BES Cyber Systems and associated Protected Cyber Assets through use of Electronic Security Perimeters; and (2) implementing remote access protection.

[46] CIP-006-6 requires Responsible Entities to: (1) set up a Physical Security Perimeter ("PSP"), restrict access into the PSP, and monitor for unauthorized access and issue alerts; and (2) establish a visitor control program (escorted access, logging).

[47] CIP-007-6 requires Responsible Entities to implement controls related to ports and services, security patch management, malicious code prevention, security event monitoring, and system access control.

[48] CIP-008-5 requires Responsible Entities to: (1) implement a cyber security incident response plan that sets forth process for identifying, classifying and responding to Cyber Security Incidents and for reporting incidents that compromise or disrupt a reliability task to E-ISAC; and (2) periodically test and update the response plan.

[49] CIP-009-6 requires Responsible Entities to: (1) implement a recovery plan to address the recovery of reliability functions performed by BES Cyber Systems; and (2) periodically test and update the response plan.

[50] CIP-010-2 requires Responsible Entities to: (1) establish a configuration change management plan to prevent and detect unauthorized changes to BES Cyber Systems; (2) conduct periodic vulnerability assessments; and (3) implement controls for use transient electronic devices to prevent the spread of malicious code.

[51] CIP-011-2 requires Responsible Entities to implement controls to protection BES Cyber Security Information.

Incident response. Proposed Reliability Standard CIP-003-7, which is pending before the Commission in Docket No. RM17-11-000, would add a fifth subject matter – protection of transient electronic devices – applicable to low impact BES Cyber Systems.[52]

The SDT chose to rely on the existing risk-based framework in the CIP Reliability Standards and applied the requirements in the proposed Reliability Standards only to high and medium impact BES Cyber Systems as they are consistent with the type of existing CIP cybersecurity requirements applicable to high and medium impact BES Cyber Systems as opposed to those applicable to low impact BES Cyber Systems. Prioritizing high and medium impact BES Cyber Systems in the new supply chain risk management requirements appropriately focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed Reliability Standards prioritize high and medium impact BES cyber systems by specifying mandatory requirements applicable to such systems, while affording entities the flexibility to determine appropriate supply chain cybersecurity risk management steps for low impact BES Cyber Systems. The approach provides an opportunity for industry to address complex supply chain cybersecurity risks in a measured manner, using an established prioritization mechanism. The benefit of this approach is that it allows entities to initially focus their resources on the higher impact BES Cyber Systems, which may eventually lead to better supply chain cybersecurity risk management plans throughout the organization.

NERC anticipates, however, that Responsible Entities with high or medium impact BES Cyber Systems may also apply their supply chain cybersecurity risk management plans to low

[52] In short, for low impact BES Cyber Systems, CIP-003-7 would require entities to: (1) reinforce cyber security practices once every 15 months; (2) control physical access to low impact BES Cyber Systems; (3) permit only necessary inbound and outbound electronic access (or authenticate Dial-up Connectivity) to the low impact BES Cyber; (4) have a Cyber Security Incident response plan; and (5) apply protections to transient electronic devices connected to BES Cyber Systems.

impact BES Cyber Systems. During development of the proposed Reliability Standard, entities commented that many of the same vendors supply products and services for all three impact categories and that the same products and services are procured for all three impact categories without differentiation. As such, by requiring that entities implement supply chain cybersecurity risk management plans for high and medium impact BES Cyber Systems, those plans would likely also cover their low impact BES Cyber Systems. Entities may decide not to establish two separate processes for the procurement of products and services for BES Cyber Systems based on impact level, either because during the planning and procurement phase they may not know which environment that system will be placed or simply because it is organizationally more efficient to have a single process for planning and procuring all BES Cyber Systems. Additionally, as Responsible Entities implement their supply chain cybersecurity risk management plans, the vendor community serving the electric industry may respond by including certain security concepts in product design and as standard provisions in future contracts for BES Cyber Systems, regardless of impact level. In this manner, implementation of proposed Reliability Standard CIP-013-1 could enhance the security for all BES Cyber Systems, not just those to which the Reliability Standard specifically applies.

The SDT also excluded Physical Access Controls ("PACS"), Electronic Access Control and Monitoring Systems ("EACMS"), and Protected Cyber Assets ("PCAs") from the scope of the proposed Reliability Standards, with the exception of the modifications in proposed Reliability Standard CIP-005-6, which also apply to PCAs. While certain of the requirements in the existing CIP Reliability Standards require Responsible Entities to apply certain protections to PACS, EACMS, and PCAs, given their association with BES Cyber Systems (either by function or location), the SDT determined that for purposes of proposed Reliability Standard CIP-013-1 and

the modifications in proposed Reliability Standard CIP-010-3, the requirements should focus on high and medium impact BES Cyber Systems only. High and medium impact BES Cyber Systems directly impact Real-time operations and, in turn, present the greatest level of risk to reliable operations. As with the exclusion of low impact BES Cyber Systems, the SDT concluded that applying the proposed supply chain risk management requirements to PACS, EACMS, and PCAs would divert resources from protecting medium and high BES Cyber Systems.

Nevertheless, NERC expects that many of these Cyber Assets would be subject to the supply chain risk management plans required by proposed Reliability Standard CIP-013-1. Registered Entities may implement a single process for procuring products and service associated with their operational environments. Further, registered entities may also use the same vendors for procuring PACS, EACMS, and PCAs as they do for high and medium impact BES Cyber Systems such that the same security considerations may be addressed for those Cyber Assets.

NERC will continue studying supply chain risks to determine whether the proposed Reliability Standards are appropriately scoped to mitigate those risks. In the series of resolutions the NERC Board issued when adopting the proposed Reliability Standards, the Board requested that:

> (i) NERC management, in collaboration with the appropriate NERC technical committees, industry representatives and appropriate experts, including representatives of industry vendors, further study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified, and (ii) NERC management provide an interim report to the Board related to the foregoing by no later than approximately 12 months after the adoption of these resolutions and a follow-up final report to the Board no later than approximately 18 months after the adoption of these resolutions.

Accordingly, over the next 18 months, NERC, working with various stakeholders, will continue to assess whether supply chain risks related to low impact BES Cyber Systems, PACS, EACMS, and PCA necessitate further consideration for inclusion in a mandatory Reliability Standard.

3) Applicable Third-Party (Vendor) Products and Services

Proposed Reliability Standard CIP-013-1 and the proposed modifications in Reliability Standard CIP-005-6, Requirement R2 apply to interactions with "vendors." As used in these proposed Reliability Standards, the term "vendor" is used broadly to refer to any person, company, or other organization with whom the Responsible Entity, or an affiliate, contracts with to supply BES Cyber Systems and related services to the Responsible Entity. A vendor, as used in the standard, may thus include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators. The use of the term "vendor," however, was not intended to bring within the scope of these proposed Reliability Standards registered entities that provide reliability services to other registered entities as part of their functional obligations under NERC's Reliability Standards (e.g., a Balancing Authority providing balancing services for registered entities in its Balancing Authority Area).

4) Applicable Vendor Contracts

Implementation of the requirements in the proposed Reliability Standards do not require Responsible Entity's to renegotiate or abrogate existing contracts with vendors executed as of the effective date of the proposed Reliability Standards. As noted above, in Order No. 829, the Commission directed NERC to develop a "forward-looking" Reliability Standard. As the Commission explained in its Notice of Proposed Rulemaking leading to Order No. 829, a "forward-looking" Reliability Standard is one that does not dictate the abrogation or re-negotiation

of currently-effective contracts with vendors.[53] As such, the requirements to develop and implement supply chain risk management plans according to CIP-013-1 apply only to new arrangements with vendors for BES Cyber Systems.[54] Responsible Entities need not apply their supply chain risk management plans to the acquisition of applicable vendor products or services pursuant to contracts executed prior to the effective date of CIP-013-1 nor would such contracts need to be renegotiated or abrogated to comply with the proposed Reliability Standard. Additionally, and consistent with the development of a "forward looking" Reliability Standard, if entities are in the middle of procurement activities for an applicable product or service at the time of the effective date of proposed Reliability Standard CIP-013-1, NERC would not expect entities to begin those activities anew to implement their supply chain cybersecurity risk management plan to comply with proposed Reliability Standard CIP-013-1.

Similarly, Responsible Entities may implement the new requirements in proposed CIP-005-6 and CIP-010-1 without renegotiating or abrogating existing contracts. Nothing in those requirements require that entities renegotiate or abrogate existing contracts.[55]

### C. Proposed Requirements of Proposed Reliability Standard CIP-013-1

The focus of proposed Reliability Standard CIP-013-1, and the development and implementation of supply chain cybersecurity risk management plans in particular, is on the steps Responsible Entities take to consider and address cyber security risks from vendor products or services during BES Cyber System planning and procurement. Given the (i) differences in the

---

53 *Revised Critical Infrastructure Protection Reliability Standards*, 152 FERC ¶ 61,054, at P 64 (2015).

54 Requirement R2 of proposed Reliability Standard CIP-013-1 specifically includes a note that implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders).

55 New Part 1.6 of proposed Reliability Standard CIP-010-3 specifically includes a note that implementation does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders).

needs and characteristics of registered entities and (ii) diversity of BES environments, technologies, and risks, proposed Reliability Standard CIP-013-1 does not impose any specific controls nor mandate "one-size-fits-all" requirements, consistent with Order No. 829.[56] The goal is to help ensure that Responsible Entities establish organizationally-defined processes that integrate a cybersecurity risk management framework into the system development life cycle.

Proposed Reliability Standard CIP-013-1 includes the following three requirements, each of which is discussed below:

> **R1.** Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]
>
> **1.1.** One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
>
> **1.2.** One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:
>
> **1.2.1.** Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
>
> **1.2.2.** Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;
>
> **1.2.3.** Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;
>
> **1.2.4.** Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

[56] Order No. 829 at P 2.

**1.2.5.** Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and

**1.2.6.** Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

**R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

**R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

Requirement R1 mandates that each Responsible Entity develop a supply chain cybersecurity risk management plan for high and medium impact BES Cyber Systems. These plans are designed to ensure that Responsible Entities: (1) adequately consider security risks when planning for high and medium impact BES Cyber Systems (Part 1.1); and (2) take steps to address relevant security concepts in future contracts for high and medium impact BES Cyber Systems (Part 1.2).

Specifically, pursuant to Part 1.1, Responsible Entities must have a process to identify and assess cybersecurity risks to the BES from vendor products and services, related to both the procurement and installation of vendor products as well as transitioning between vendors. This obligation addresses the third objective outlined in Order No. 829 to address a Responsible Entity's "identification and documentation of the risks of proposed information system planning and system development actions."[57] As the Commission stated in Order No. 829, this "objective addresses "the risk that [R]esponsible [E]ntities could unintentionally plan to procure and install unsecure equipment or software within their information systems, or could unintentionally fail to

[57] *Id*. at P 56.

anticipate security issues that may arise due to their network architecture or during technology and vendor transitions."

Requiring entities to identify and assess cybersecurity risks during the planning phase of the system life cycle helps ensure that Responsible Entities make informed decisions by adequately considering the cybersecurity risks presented by a particular vendor, product, or service, as well as available options for mitigating any such risks. Based on the identification and assessment of risks, the Responsible Entity may choose not to move forward with a particular vendor or product or, if it chooses to move forward, implement targeted mitigation measures to harden its BES Cyber System, minimize the attack surface, ensure ongoing support for system components, and identify alternate sources for critical components, among other things.

Pursuant to Part 1.2, Responsible Entities must also have processes to address the following baseline set of security concepts in their procurement activities for high and medium impact BES Cyber Systems: (1) vendor security event notification processes (Part 1.2.1); (2) coordinated incident response activities (Part 1.2.2); (3) vendor personnel termination notification for employees with access to remote and onsite systems (Part 1.2.3); (4) product/services vulnerability disclosures (Part 1.2.4); (5) verification of software integrity and authenticity (Part 1.2.5); and (5) coordination of vendor remote access controls (Part 1.2.6). Part 1.2 addresses the fourth objective outlined in Order No. 829 to "address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."[58]

[58] *Id*. at P 59.

Each item listed in Parts 1.2.1 through 1.2.4 corresponds to a topic specifically listed in Order No. 829 for which entities must have controls.[59] Further, Parts 1.2.5 and 1.2.6 address, together with the modifications in proposed Reliability Standards CIP-005-6 and CIP-010-3, the first and second objective discussed in Order No. 829 related to software integrity and authenticity and vendor remote access. Collectively, each of the listed items help address the risks that: (1) Responsible Entities could enter into contracts with vendors who pose significant risks to their information systems; (2) products procured by a Responsible Entity fail to meet minimum security criteria; and (3) a compromised vendor would not provide adequate notice of security issues and related incident response to Responsible Entities with whom that vendor is connected.[60] As discussed further below, the focus of Part 1.2 is not on requiring that every contract with a vendor includes provisions for each of the listed items but on developing processes to ensure that these security items are an integrated part of procurement activities (e.g., these topics are included in requests for proposals ("RFPs") or the contract negotiation process).

Requirement R2 mandates that each Responsible Entity implement its supply chain cybersecurity risk management plan developed in accordance with Requirement R1. Requirement R2 also includes the following note:

> Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

As discussed above, the note that implementation of the supply chain cybersecurity risk management plans do not require the renegotiation or abrogation of existing contracts is consistent

[59] *Id*. at P 59.

[60] *Id*. at P 61.

with the Commission's statement in Order No. 829 to develop a "forward-looking" Reliability Standard.

Similarly, the note that (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract are outside the scope of proposed Reliability Standards CIP-013-1 is consistent with the directive in Order No. 829 to develop an objective-based supply chain cybersecurity risk management Reliability Standard that "account[s] for, among other things, differences in the needs and characteristics of [R]esponsible [E]ntities and the diversity of BES Cyber System environments, technologies and risks."[61] As noted above, the focus of CIP-013-1 is on the processes Responsible Entities implement to consider and address cyber security risks from vendor products or services during BES Cyber System planning and procurement, not on the outcome of those processes, such as the Responsible Entity choice of vendor for a particular product or service, the negotiated contract terms for a particular product service, or the vendor's adherence performance under the contract to implement the various security provisions agreed to by the parties). Those outcomes are more appropriately left to the discretion of the Responsible Entity.

Proposed Reliability Standard CIP-013-1 must be flexible enough to account for the significant differences in the purchasing power and resource needs of various Responsible Entities and balance the reliability need to implement supply chain management security controls with a Responsible Entities' business need to obtain products and services at a reasonable cost. A Responsible Entity may not have the ability to obtain each of its desired cybersecurity controls in its contract with each of its vendors. Factors such as competition, limited supply sources, expense, criticality of the product or service, and maturity of the vendor or product line could affect the

[61] *Id*. at P 44.

terms and conditions ultimately negotiated by the parties and included in a contract. After weighing the risks associated with a vendor or product and making a good faith effort to include security controls in any agreement with a vendor, as required by proposed CIP-013-1, Responsible Entities must make a business decision on whether and how to proceed. Variation in contract terms is thus anticipated and, in turn, the note in Requirement R2 provides that the actual terms and conditions of the contract are outside the scope of Reliability Standard CIP-013-1.

Similarly, a vendor's performance under its contract with a Responsible Entity should remain outside the scope of the proposed Reliability Standard. While NERC expects Responsible Entities to enforce the security provisions in its vendor contracts, a Responsible Entity should not be held responsible under the proposed Reliability Standard for actions (or inactions) of the vendor. The aim of the proposed Reliability Standard is to create an affirmative obligation for Responsible Entities to implement supply chain cybersecurity risk management controls without holding them strictly liable for the actions of its vendors. There are many factors (e.g., risk assessment, relationship with counterparty, cost, etc.) that go into a decision to enforce contract provisions against the counterparty. Such decisions are not susceptible to a one-size-fits-all mandate in a mandatory Reliability Standard. As such, the note in Requirement R2 provides that vendor performance and adherence to a contract are outside the scope of proposed Reliability Standard CIP-013-1.

Accordingly, failure to obtain a specific contract provision for an item listed in Part 1.2, or the failure to enforce a security provision in a vendor contract would not constitute a violation of Requirements R1 or R2 of proposed Reliability Standard CIP-013-1. In assessing compliance with the proposed Reliability Standard, the ERO would focus on whether the Responsible Entity: (1) developed processes reasonably designed to (i) identify and assess risks associated with vendor

products and services in accordance with Part 1.1, and (ii) ensure that the security items listed in Part 1.2 are an integrated part of procurement activities; and (2) implemented those processes in good faith. On the latter element, the ERO will evaluate the steps Responsible Entity's took, in accordance with its supply chain cybersecurity risk management plan, to assess risks posed by a vendor and associated products or services and, based on that risk assessment, the steps the entity took to mitigate those risk, including the negotiation of security provisions in its agreements with the vendor.

Consistent with the Commission statement that "the Reliability Standard should set goals (the "what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how")," Requirements R1 and R2 of proposed CIP-013-1 provides Responsible Entities flexibility to develop and implement processes that best suits the needs and characteristics of their organization, and the BES system environments to which a vendor product or service relates. To assist with the implementation of proposed Reliability Standard CIP-013-1, the SDT developed an Implementation Guidance document, endorsed by the ERO consistent with its Compliance Guidance Policy,[62] which outlines various approaches to implementing proposed Reliability Standard CIP-013-1. That Implementation Guidance provides, among other things, that in developing and implementing its supply chain cybersecurity risk management plan, a Responsible Entity may consider using a risk-based approach that identifies and prioritizes security controls based on the cybersecurity risks presented by the vendor and the criticality of the product or service to reliable operations. For instance, Responsible Entities may establish a baseline set of controls for given products or services that a vendor must meet prior to

[62] The SDT's Implementation Guidance is provided in Exhibit E hereto. The ERO's Compliance Guidance Policy is available at http://www.nerc.com/pa/comp/Resources/ResourcesDL/Compliance_Guidance_Policy_FINAL_Board_Accepted_Nov_5_2015.pdf.

transacting with that vendor for those products and services (i.e., "must-have controls"). As risks differ between products and services, the baseline security controls – or "must haves" – may differ for the various products and services that the Responsible Entity procures for its BES Cyber Systems. This risk-based approach could help create efficiencies in the Responsible Entity's procurement processes while meeting the security objectives of Requirement R1.

Additionally, for Requirement R1, the Implementation Guidance outlines two basic approaches for developing supply chain cybersecurity risk management plans:

> One element of, or approach to, a risk-based cyber security risk management plan is system-based, focusing on specific controls for high and medium impact BES Cyber Systems to address the risks presented in procuring those systems or services for those systems. A risk-based approach could also be vendor-based, focusing on the risks posed by various vendors of its BES Cyber Systems. Entities may combine both of these approaches into their plans.

The Implementation Guidance provides additional detailed considerations for implementing the requirements in proposed Reliability Standard CIP-013-1 and examples of approaches that Responsible Entities could use to meet the requirements.

Requirement R3 of proposed Reliability Standard CIP-013-1 addresses the Order No. 829 directives to require each Responsible Entity to periodically reassess its supply chain cyber security risk management controls.[63] Under Requirement R3, the Responsible Entity shall review and obtain its CIP Senior Manager's (or delegate's) approval of its supply chain risk management plan at least once every 15 calendar months. This 15-month assessment helps ensure that the supply chain cybersecurity risk management plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.

[63] Order No. 829 at P 46.

### D. Proposed Modifications in Reliability Standard CIP-005-6

Proposed Reliability Standard CIP-005-6 includes two new parts in Requirement R2 – Part 2.4 and 2.5 – to address the second objective discussed in Order No. 829 regarding vendor remote access sessions.[64] Parts 2.4 and 2.5 apply to medium and high impact BES Cyber Systems and their associated PCAs and provide as follows:

> **2.4** Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
>
> **2.5** Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

These new requirement parts work in tandem with Requirement R1 Part 1.2.6 of proposed Reliability Standard CIP-013-1 to address vendor remote access. As discussed above, Requirement R1 Part 1.2.6 of proposed CIP-013-1 creates an affirmative obligation during procurement activities for Responsible Entities to address the coordination of controls with the vendor for Interactive Remote Access and system-to-system remote access. Parts 2.4 and 2.5 of proposed CIP-005-6 complement that obligation by creating affirmative obligations in the operational phase for Responsible Entities to have one or more methods for: (1) determining active vendor remote access sessions (Part 2.4); and (2) disabling active vendor remote access (Part 2.5). The security objective of these requirement parts is to control vendor remote access to mitigate risks associated with unauthorized access (i.e., reduce the probability that an attacker could use legitimate third-party access to compromise Responsible Entity systems).

More specifically, the objective of Part 2.4 is for entities to have visibility into all active vendor remote access sessions (both Interactive Remote Access and system-to-system remote access) that are taking place on their system. The objective of Requirement R2 Part 2.5 is for

---

64 *Id*. at P 51.

entities to have the ability to disable active remote access sessions in the event of a system breach. Visibility into vendor remote access sessions and the capability to rapidly disable such sessions will help prevent unauthorized access and the type of cyberattack that successfully affected the Ukraine's power grid in 2015.[65]

In addition to adding Parts 2.4 and 2.5 to the Reliability Standard, NERC modified Requirement R2 to only reference Interactive Remote Access where appropriate. With the exception of proposed Parts 2.4 and 2.5, Requirement R2 applies only to Interactive Remote Access, not system-to-system remote access. Accordingly, the phrase "allowing Interactive Remote Access to BES Cyber Systems" was removed from the introductory sentence of Requirement R2 but the phrase "For all Interactive Remote Access," was included in Part 2.1.

NERC also made other clean-up changes in the proposed CIP-005-6 Reliability Standard, including changes to the standard so as to be consistent with NERC's newer template, and deleting from the Applicability Section of the standard references to Special Protection System ("SPS"), which is now defined to refer to the Remedial Action Scheme ("RAS") definition.[66] The Applicability Section of the proposed Reliability Standard now references RAS only.

### E. Proposed Modifications in Reliability Standard CIP-010-3

Proposed Reliability Standard CIP-010-6 includes a new part in Requirement R1 – Part 1.6 – to address the first objective discussed in Order No. 829 regarding verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and (2) the integrity of the software and patches before they are installed in the BES

---

65 *See* E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid* at 3 (Mar. 18, 2016), http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

66 See Order No. 818, *Revisions to Emergency Operations Reliability Standards; Revisions to Undervoltage Load Shedding Reliability Standards; Revisions to the Definition of "Remedial Action Scheme" and Related Reliability Standards*, 153 FERC ¶ 61,228 (2015); Letter Order, *North American Electric Reliability Corporation*, Docket No. RD16-5-000 (Jun. 23, 2016).

Cyber System environment.[67] Consistent with that objective, Requirement R1 Part 1.6 of proposed Reliability Standard CIP-010-3 provides:

> **1.6** Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:
>
> 1.6.1. Verify the identity of the software source; and
>
> 1.6.2. Verify the integrity of the software obtained from the software source.

Essentially, Part 1.6 provides that prior to installing software that changes the established baseline configuration for (1) operating system(s) (including version) or firmware where no independent operating system exists (Part 1.1.1), (2) any commercially available or open-source application software (including version) intentionally installed (Part 1.1.2), or (3) any custom software installed (Part 1.1.3), Responsible Entities must verify the identity of the software source and the integrity of the software obtained by the software sources, when methods are available to do so. The security objective of verifying software integrity and authenticity is to ensure that the software being installed in the BES Cyber System was not modified without the awareness of the software supplier and is not counterfeit. These steps, as the Commission stated in Order No. 829, help "reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System."[68]

As with Parts 2.4 and 2.5 of proposed CIP-005-6, proposed Part 1.6 works in tandem with Requirement R1 Part 1.2.5 of proposed CIP-013-1 to address software integrity and authenticity. As discussed above, Requirement R1 Part 1.2.5 of proposed CIP-013-1 creates an affirmative obligation during procurement activities for Responsible Entities to address the verification of

---

[67] Order No. 829 at P 48.

[68] *Id.* at P 49.

software integrity and authenticity for all software and patches provided by the vendor for use in a BES Cyber System. Part 1.6 of proposed CIP-010-3 complements that obligation by creating an affirmative obligation in the operational phase for Responsible Entities to verify software integrity and authenticity. The obligation to verify software integrity and authenticity, however, can only be accomplished if the source of the software provides a method to do so. Hence, it is important for entities to address this matter in their procurement activities, as required by CIP-013-1.

In addition to adding Part 1.6 to the Reliability Standard, NERC also made other clean-up changes, including changes to the standard so as to be consistent with NERC's newer template, and deleting from the Applicability Section of the standard references to SPS, which is now defined to refer to the RAS definition as noted above. The Applicability Section of the proposed Reliability Standard now references RAS only.

### F. Enforceability of Proposed Reliability Standards

The proposed Reliability Standards also include 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.[69] Additionally, the proposed Reliability Standards include VRFs and VSLs. The VRFs and VSLs provide guidance on the way that NERC will enforce the requirements of the proposed Reliability Standards. The VRFs and VSLs for the proposed Reliability Standards comport with NERC and Commission guidelines related to their assignment. Exhibit F provides a detailed review of the VRFs and VSLs, and the analysis of how the VRFs and VSLs were determined using these guidelines.

[69] Order No. 672 at P 327.

## V. EFFECTIVE DATE

NERC respectfully requests that the Commission approve the proposed Reliability Standards to become effective as set forth in the proposed Implementation Plan, provided in Exhibit B hereto. The proposed Implementation Plan provides that the proposed Reliability Standards shall become effective on the first day of the first calendar quarter that is 18 calendar months after the effective date of the Commission's order approving the proposed Reliability Standard. The 18-month implementation period is designed to afford Responsible Entities sufficient time to develop and implement their supply chain cybersecurity risk management plans according to proposed Reliability Standard CIP-013-1 and implement the new controls required in proposed Reliability Standards CIP-005-6 and CIP-010-3.

## VI. ACTIVITIES TO SUPPORT IMPLEMENTION OF THE PROPOSED RELIABILITY STANDARDS AND ADDRESS RESIDUAL RISKS

In addition to directing NERC management to further study the nature and complexity of cyber security supply chain risks, as discussed above, as part of the resolutions it issued when adopting the proposed Reliability Standards, the Board directed NERC management to take a number of steps to support successful implementation of the proposed Reliability Standards. Specifically, the Board directed NERC management to do the following:

- "[C]ommence appropriate preparations for implementation of the Supply Chain standards utilizing methods similar to those utilized for the implementation of the CIP v 5 reliability standards as deemed appropriate by NERC management, and regularly report to the Board on such activities."

- "[U]tilizing information it is authorized to use and other information collected through interactions with industry and governmental authorities, communicate supply chain risk developments and risks to industry and in connection with the efforts contemplated by the foregoing resolutions."

The Board also requested that certain stakeholder groups take certain actions to support implementation activities. Specifically, the Board requested the following:

- "[T]hat each of the North American Transmission Forum and the North American Generation Forum (the "Forums") develop white papers to address best and leading practices in supply chain management, including procurement, specifications, vendor requirements and existing equipment management, that are shared across the membership of each Forum, and to the extent permissible under any applicable confidentiality requirements, distribute such white papers to industry."

- "[T]hat the Board hereby requests that each of the National Rural Electric Cooperative Association and the American Public Power Association (the "Associations") develop white papers addressing issues contemplated by the immediately preceding resolution, focusing on smaller entities that are not members of the Forums, for the membership of the Associations, and to the extent permissible under any applicable confidentiality requirements, distribute such white papers to industry.

The Board also requested that "NERC management, collaborating with the appropriate NERC technical committees and other experts as deemed appropriate by management, develop a plan to evaluate the effectiveness of the Supply Chain Standards, including seeking input from registered entities subject to the Supply Chain Standards, and report back to the Board as appropriate."

Consistent with the Board's resolutions, NERC is planning a number of coordinated activities to support (i) industry's implementation of the proposed Reliability Standards and (ii) broader efforts to address and mitigate supply chain cybersecurity risks. The purpose of these activities is to accomplish the following objectives, among others: (1) enhancing industry's readiness to implement the Reliability Standards; (2) clarifying compliance and enforcement expectations; (3) ensuring consistent and reasonable enforcement of the proposed Reliability Standards; (4) assessing the effectiveness of the proposed Reliability Standards in mitigating supply chain cybersecurity risks; (5) fostering increased analysis and information sharing of supply chain cybersecurity threats and vulnerabilities and risk management best practices; and (6) promoting programs within the electric industry designed to identify supply chain cybersecurity threats and vulnerabilities and enhance supply chain risk management activities. NERC will

engage directly with registered entities, the vendor community, and relevant governmental entities, among others, to accomplish these objectives.

In its plans to support implementation of the proposed Reliability Standards, NERC is drawing on its past initiatives and lessons learned in support of the transition to other significant sets of Reliability Standards, particularly the transition to the CIP Reliability Standards approved in Order Nos. 791 and 822,[70] commonly referred to as the CIP version 5 Reliability Standards. NERC's early engagement in supporting transition to the CIP version 5 Reliability Standards helped identify and address implementation issues to support an efficient and effective transition. For the proposed Reliability Standards, NERC plans the following types of activities beginning in the fourth quarter of 2017 and continuing into 2018 and beyond:

- *Implementation Study and Advisory Task Force* – Drawing from lessons learned from the transition to the CIP version 5 Reliability Standards, NERC plans to identify and solicit a core group of volunteer registered entities with mature supply chain risk management practices to participate in an implementation study and serve on an advisory task force to provide feedback on Reliability Standard application successes and challenges, identify needed enhanced Implementation Guidance, and share best practices. Specifically, NERC plans to collaborate with select registered entities during their implementation of the proposed Reliability Standards to better understand and assess the effectiveness of those Supply Chain standards (and associated Implementation Guidance) at mitigating supply chain cybersecurity risks. A central focus of this initiative will be to measure the impact and influence that the proposed Reliability Standards have in shaping supply chain cybersecurity risk management behaviors and practices across the electric industry. This initiative will also evaluate the manner in which vendors have responded to registered entities' implementation of the proposed Reliability Standards.

- *Auditor Training* – To help ensure consistent application of the proposed Reliability Standards, NERC will focus on Regional Entity auditor training on the concepts in the proposed Reliability Standards along with application of associated Implementation Guidance, focusing on acceptable approaches to compliance. Auditor training would be informed by the lessons learned from the implementation study and the advisory task force.

- *Outreach and Communication* – NERC plans to increase outreach and communication with industry stakeholders to help ensure implementation readiness, including periodic

[70] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014); *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037 (2016).

webinars, small registered entity outreach, and other activities to align industry and Regional Entity understanding on compliance approaches.

- *CIPC Guidance* – NERC plans to engage the Critical Infrastructure Protection Committee ("CIPC") and other qualified groups to develop additional Implementation Guidance, as needed.

- *Monitoring and Oversight* – During implementation of the proposed Reliability Standards, NERC will continue to develop oversight strategies to monitor compliance and assess the effectiveness of the proposed Reliability Standards in helping to mitigate supply chain cybersecurity risks to the BES.

- *Vendor Engagement* – NERC plans to engage with the vendor community with a focus on supply chain risk management controls.

Collectively, NERC expects that these types of initiatives will help: the identification and sharing of supply chain cybersecurity risk management best practices to enhance industry's implementation readiness; validate existing guidance related to the proposed Reliability Standards; identify areas that may need additional or enhanced guidance; promote increased awareness among vendors of industry's needs in meeting the proposed Reliability Standards; measure the impact of the proposed Reliability Standards on supply chain cybersecurity risk management practices; and evaluate whether the Supply Chain Standards adequately address identified or emerging supply chain cybersecurity risks

Additionally, NERC is committed to using its many reliability tools – e.g., guidelines, training exercises, alerts, information sharing and analysis – to further study and assess supply chain cybersecurity risks and support the electric industry's efforts to mitigate supply chain risks outside of the context of compliance with the proposed Reliability Standards. Specifically, NERC plans to initiate the following types of activities to promote actions that will address residual supply chain cybersecurity risks:

- NERC plans to work with CIPC and other technical committees to develop guidelines that identify best practices, internal controls, as well as processes and concepts that can be shared amongst registered entities to promote strong supply chain cybersecurity risk management for all BES Cyber Systems. The guidelines would include legacy system

support for end-of-life products and the use of resellers or third-party suppliers for BES Cyber System components.

- NERC will explore opportunities to engage the vendor community through joint industry/vendor working groups and targeted outreach (e.g. EMS vendor user groups) to identify and address emerging supply-chain risks, as well as discuss system development activities and security vulnerability identification processes.

- NERC plans to review supply chain standards and other similar guidance documents prepared by other standards setting organizations to gain additional insight for best practices. NERC will share lessons learned from inside and outside the industry with registered entities.

- NERC will consider integrating a supply chain vulnerability in the next GridEx exercise, including a post mortem analysis of the response efforts from entities.

- NERC will explore opportunities to engage trade organizations to educate industry about effective strategies for enhancing the reliability and security of supply chains, in addition to the Board's request that the Forums and Associations develop white papers.

- NERC, primarily through the Electricity Information Sharing and Analysis Center ("E-ISAC"), will explore opportunities to engage governmental entities such as the Department of Homeland Security ("DHS") and the Department of Energy (DOE) on an overarching strategy for addressing supply chain risks.

- NERC, primary through the E-ISAC, will continue to analyze and share information related to supply chain threats and vulnerability and approaches to timely mitigate those threats and vulnerabilities to help ensure the electric industry has situation awareness of and remains focused on supply chain issues.

- NERC will explore opportunities to engage the DOE National Laboratories and other relevant organizations to encourage them to identify and share system vulnerability information to the asset owner and vendor community. For example, NERC, in coordination with the CIPC and other stakeholder groups, will explore opportunities to work with the National Laboratories to test equipment and systems used by registered entities in their operational environments to further assess whether cybersecurity vulnerabilities exist in installed equipment or systems. The results of these tests would be shared with applicable asset owners and vendors.

- NERC will explore opportunities to engage the Institute of Electrical and Electronics Engineers, Internet Engineering Task Force, International Electrotechnical Commission, and other product manufacturing standards bodies to ensure that supply chain cybersecurity risks and vulnerabilities are addressed in standard product specifications.

- NERC will explore opportunities to assist stakeholders in developing an accreditation model for identifying vendors with strong supply chain risk management practices. Such identification would not only help entities comply with the proposed Reliability Standards

but also increase the level of confidence that vendors providing BES-related products and services are effectively implementing supply chain cybersecurity controls and measures.

Through these or other similar activities, NERC, in coordination with its stakeholders, intends to proactively address supply chain threats and vulnerabilities that could impact BES reliability. The proposed Reliability Standards are one element of NERC's efforts to increase focus on supply chain-related cybersecurity risks and improve the cybersecurity practices in the electric industry.

## VII. CONCLUSION

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

- proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3, and associated elements included in Exhibit A, effective as proposed herein;
- the proposed Implementation Plan included in Exhibit B; and
- the retirement of Reliability Standards CIP-005-5 and CIP-010-2, effective as proposed herein.

Respectfully submitted,

*/s/ Shamai Elstein*

Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net

*Counsel for the North American Electric Reliability Corporation*

Date: September 26, 2017