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

Exhibit A

Proposed Reliability Standards

Exhibit A

Proposed Regional Reliability Standard

CIP-005-6 – Cyber Security – Electronic Security Perimeter(s)

Clean

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-6:

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

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002 identification and categorization processes.
- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.

- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-6 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-6 Table R2 – Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5).	Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

Exhibit A

Proposed Regional Reliability Standard

CIP-005-6 – Cyber Security – Electronic Security Perimeter(s)

Redline

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-~~5~~6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~5:~~ 6:

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

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

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

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

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

5. ~~5.~~ Effective Date~~s~~:

~~1. **24 Months Minimum –** CIP-005-5 shall become effective on the later of July 1, 2015, or the first calendar day of the ninth calendar quarter after the effective date of the order providing applicable regulatory approval.~~

~~2. In those jurisdictions where no regulatory approval is required, CIP-005-5 shall become effective on the first day of the ninth calendar quarter following Board of Trustees' approval, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.~~

~~6.~~ See Implementation Plan for Project 2016-03.

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

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

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

- **High Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to high impact BES Cyber Systems with Dial-up Connectivity.
- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to ~~each~~ BES Cyber Systems categorized as medium impact according to the CIP-002~~-5~~ identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~5~~6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~5~~6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~5~~6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-~~5~~6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

~~CIP-005-5 Table R1 – Electronic Security Perimeter~~			
~~Part~~	~~Applicable Systems~~	~~Requirements~~	~~Measures~~
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

R2. Each Responsible Entity ~~allowing Interactive Remote Access to BES Cyber Systems~~ shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-~~5~~6 Table R2 – ~~Interactive~~ Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~5~~6 Table R2 – ~~Interactive~~ Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~5~~6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	~~Utilize~~For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-~~5~~6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-~~5~~6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-~~5~~6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. **Compliance Monitoring Process~~:~~**

~~1.1.~~ Compliance Enforcement Authority:

1.1. ~~The Regional Entity shall serve as the~~ "Compliance Enforcement Authority ~~("CEA") unless the applicable~~" means NERC or the Regional Entity, or any entity ~~is owned, operated, or controlled~~as otherwise designated by ~~the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC~~ an Applicable Governmental Authority, in their respective roles of monitoring and/or ~~other applicable governmental authority shall serve as the CEA~~enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention ~~periods~~period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~CEA~~Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

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

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

~~1.2. Compliance Monitoring and Assessment Processes:~~

- ~~Compliance Audit~~
- ~~Self-Certification~~
- ~~Spot Checking~~
- ~~Compliance Investigation~~
- ~~Self-Reporting~~
- ~~Complaint~~

~~1.3. Additional Compliance Information:~~

- ~~None~~

~~**2. Table of Compliance Elements**~~

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-005-5)~~				
			Lower VSL	Moderate VSL		High VSL	Severe VSL
R1.			~~Operations Planning and Same Day Operations~~	~~Medium~~		The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-~~5~~6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-005-5)~~				
			Lower VSL	Moderate VSL		High VSL	Severe VSL
							was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-5)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	Operations Planning and Same Day Operations	Medium	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3-; OR	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3-; OR

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-005-5)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

~~E. Interpretations~~

~~None.~~

~~F.~~E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
6	08/10/17	Adopted by the NERC Board of Trustees.	

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

CIP-005-~~5~~6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale~~:~~

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

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

.

~~Version History~~Version	~~Date~~	~~Action~~	~~Change Tracking~~
~~1~~	~~1/16/06~~	~~R3.2 — Change "Control Center" to "control center."~~	~~3/24/06~~
~~2~~	~~9/30/09~~	~~Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards.~~ ~~Removal of reasonable business judgment.~~ ~~Replaced the RRO with the RE as a responsible entity.~~ ~~Rewording of Effective Date.~~ ~~Changed compliance monitor to Compliance Enforcement Authority.~~	
~~3~~	~~12/16/09~~	~~Updated version number from 2 to 3~~ ~~Approved by the NERC Board of Trustees.~~	
~~3~~	~~3/31/10~~	~~Approved by FERC.~~	
~~4~~	~~12/30/10~~	~~Modified to add specific criteria for Critical Asset identification.~~	~~Update~~

4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	

Exhibit A

Proposed Regional Reliability Standard

CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments

Clean

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	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.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	

CIP-010-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

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

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This 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. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The 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.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the

SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Exhibit A

Proposed Regional Reliability Standard

CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments

Redline

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-~~2~~3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-~~2:~~ 3:

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

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

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

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

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

5. ~~5.~~ Effective Date~~s~~:

See Implementation Plan for ~~CIP-010-2~~Project 2016-03.

6. ~~6.~~ Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~2~~3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~2~~3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~2~~3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-23 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-~~2~~ 3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-~~2~~ 3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-~~2~~3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	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.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~2~~3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. ~~**M2.**~~ Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~2~~3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~2~~3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-~~2~~3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. ~~**M3.**~~ Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-~~2~~3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-~~2~~3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-23 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-~~2~~ – ~~3~~ – Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. ~~**M4.**~~ Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. **Compliance Monitoring Process~~:~~**

~~1.1.~~ Compliance Enforcement Authority:

1.1. ~~As defined in the NERC Rules of Procedure,~~ "Compliance Enforcement Authority" ~~(CEA)~~ means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with ~~the NERC~~mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention ~~periods~~period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the ~~CEA~~Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

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

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

1.3 Compliance Monitoring and Assessment Processes: ~~Compliance Audits~~

~~Self-Certifications~~

~~Spot Checking~~

~~Self-Reporting~~

~~Complaints~~As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

1.4 Additional Compliance Information:

None

~~2. Table of Compliance Elements~~

Violation Severity Levels

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	~~Operations Planning~~	~~Medium~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						do so is available to the Responsible Entity from the software source. (1.6)
R2.	~~Operations Planning~~	~~Medium~~	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	~~Long-term Planning and Operations Planning~~	~~Medium~~	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	than 18 months, but ~~less than 21, months~~ since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	~~**Long-term Planning and Operations Planning**~~	~~**Medium**~~	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-~~2~~3, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-~~2~~3, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-~~2~~3, Requirement R4,	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-~~2~~3, Requirement R4. (R4)

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-~~2~~3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for	Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-~~2~~3, Requirement R4, Attachment 1,	Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-~~2~~3, Requirement R4, Attachment 1,	

R #	~~Time Horizon~~	~~VRF~~	Violation Severity Levels ~~(CIP-010-2)~~			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Transient Cyber Assets managed by the Responsible Entity according to CIP-010-~~2~~3, Requirement R4, Attachment 1, Section 1.2. (R4)	Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~2~~3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~2~~3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

~~E. Interpretations~~

~~None.~~

~~F.~~E. Associated Documents

~~Guideline and Technical Basis (attached).~~

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-~~2~~3. Docket No. RM15-14-000	
3	07/20/17	Modified to address certain directives in FERC Order No. 829.	Revised
3	08/10/17	Adopted by the NERC Board of Trustees.	

CIP-010-~~2~~3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

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

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-~~2~~3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This 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. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

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

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The 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.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010~~-2~~ and CIP-007~~-6~~ to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single

standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Exhibit A

Proposed Regional Reliability Standard

CIP-013-1 – Cyber Security - Supply Chain Risk Management

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

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

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

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

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

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;

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).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

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.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

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. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

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

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within

	so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES 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); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

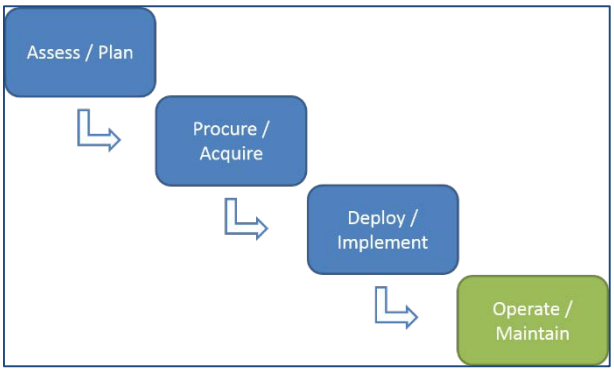
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the

awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

Exhibit B

Implementation Plan

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard

Applicable Standard(s)

CIP-005-6 — Cyber Security — Electronic Security Perimeters

CIP-010-3 — Configuration Change Management and Vulnerability Assessments

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

CIP-005-5 — Cyber Security — Electronic Security Perimeters

CIP-010-2 — Configuration Change Management and Vulnerability Assessments

Prerequisite Standard(s)

None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
  - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator

- Transmission Operator
- Transmission Owner

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 apply only to BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing 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 Bulk Electric System (BES) operations. Order No. 829 (at P 2) states:

> [The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

FERC directed NERC to submit the new or modified Reliability Standard(s) within one year of the effective date of Order No. 829, i.e., by September 27, 2017.

General Considerations

Consistent with the directive to develop a forward-looking Reliability Standard, the implementation of Reliability Standards in Project 2016-03 do not require the abrogation or re-negotiation of contracts (including amendments to master agreements and purchase orders) with vendors, suppliers or other entities executed as of the effective date of the proposed Reliability Standards (See FERC Order No. 829, P. 36).

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-1.

Effective Date

For all Reliability Standards in Project 2016-03 — CIP-005-6, CIP-010-3, and CIP-013-1

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

CIP-013-1 Requirement R3
The initial review and approval of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement R3 must be completed on or before the effective date of CIP-013-1.

Planned or Unplanned Changes Resulting in a Higher Categorizaton

Compliance timelines with CIP-005-6, CIP-010-3, and CIP-013-1 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards.

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5 (or any subsequent version of that Reliability Standard) which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For planned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 on the update of the identification and categorization of the affected BES Cyber System.

For unplanned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 according to the following timelines, following the identification and categorization of the affected BES Cyber System.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 Months
New medium impact BES Cyber System	12 Months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 Months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 Months

Retirement Date

Standards listed in the **Requested Retirement(s)** section shall be retired immediately prior to the effective date in the particular jurisdiction in which the revised standards are becoming effective.

Exhibit C

Order No. 672 Criteria

EXHIBIT C

Order No. 672 Criteria

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

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

The proposed Reliability Standards 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, consistent with the Commission directive in Order No. 829. Specifically, 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 the 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 Reliability Standards CIP-005-6 and CIP-010-3 address specific supply chain risks related to vendor remote access and software integrity and authenticity that are not already addressed in the currently-effective CIP Reliability Standards.

---

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

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

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

The proposed Reliability Standards is clear and unambiguous as to what is required and who is required to comply, in accordance with Order No. 672. The proposed Reliability Standards apply to Balancing Authorities, certain Distribution Providers, Generator Operators, Generator Owners, Interchange Coordinators or Interchange Authorities, Reliability Coordinators, Transmission Operators, and Transmission Owners. Proposed Reliability Standard CIP-013-1 does not apply to Interchange Coordinators or Interchange Authorities. The proposed Reliability Standards clearly articulates the actions that such entities must take to comply with the standards.

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

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

---

3 Order No. 672 at PP 322, 325.

4 Order No. 672 at P 326.

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

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

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

The proposed Reliability Standards achieve the reliability goals effectively and efficiently in accordance with Order No. 672. The proposed Reliability Standards clearly articulate the security objectives that applicable entities must meet and provides entities the flexibility to tailor their processes and plans required under the standard to best suit the needs of their organization.

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

The proposed Reliability Standards do not reflect a "lowest common denominator" approach. The proposed Reliability Standards represent a significant improvement over the currently-effective cybersecurity Reliability Standards. In addition to satisfying Commission directives from Order N0. 829, the Reliability Standards as proposed include additional

---

5 Order No. 672 at P 327.

6 Order No. 672 at P 328.

7 Order No. 672 at P 329-30.

requirements for protecting against cyber-attacks to Bulk Electric System ("BES") facilities, systems, and equipment.

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

The proposed Reliability Standards apply throughout North America and do not favor one geographic area or regional model.

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

The proposed Reliability Standards have no undue negative impact on competition. The proposed Reliability Standards require the same performance by each of the applicable Functional Entities for mitigating the risk of a cybersecurity incident affecting the reliable operation of the BES. The proposed Reliability Standards do not unreasonably restrict the available transmission capability or limit use of the Bulk-Power System in a preferential manner.

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

The proposed effective date for the proposed Reliability Standards are just and reasonable and appropriately balance the urgency in the need to implement the standards against the reasonableness of the time allowed for those who must comply to develop and implement the necessary procedures software, facilities, staffing or other relevant capability.

---

8 Order No. 672 at P 331.

9 Order No. 672 at P 332.

10 Order No. 672 at P 333.

The proposed 18-month implementation period for proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 will allow applicable entities adequate time to ensure compliance with the requirements, including time to develop and implement supply chain cybersecurity risk management plans in proposed Reliability Standard CIP-013-1 and implement the new controls required in proposed Reliability Standards CIP-005-6 and CIP-010-3. The proposed effective date is explained in the proposed Implementation Plan, attached as Exhibit B.

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

The proposed Reliability Standards were developed in accordance with NERC's Commission-approved, ANSI- accredited processes for developing and approving Reliability Standards. Exhibit G includes a summary of the development proceedings, and details the processes followed to develop the proposed Reliability Standards. These processes included, among other things, comment and balloting periods. Additionally, all meetings of the drafting team were properly noticed and open to the public. The initial and additional ballots achieved a quorum and exceeded the required ballot pool approval levels.

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

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

---

[11] Order No. 672 at P 334.

[12] Order No. 672 at P 335.

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

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

[13] Order No. 672 at P 323.

Exhibit D

Consideration of Directives

Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified 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.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.* The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations". High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the

Order No. 829 Citation	Directive / Guidance	Resolution
		development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed/modified standard(s) must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve	The directive is addressed by Requirements R1, R2, and R3 of proposed CIP-013-1. Requirement R1 specifies that entities must develop, and Requirement R2 specifies that entities must implement, one or more documented supply chain cyber security risk

Order No. 829 Citation	Directive / Guidance	Resolution
	these four objectives but have the flexibility as to how to reach the objective (i.e., 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")).	management plan(s) for high and medium impact BES Cyber Systems that include one or more process(es) for mitigating cyber security risks to BES Cyber Systems. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle. **Proposed CIP-013-1 Requirement R1** **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: **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

Order No. 829 Citation	Directive / Guidance	Resolution
		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; **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). **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require 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. This periodic assessment should better ensure	The directive is addressed in proposed CIP-013-1 Requirement R3. **Proposed CIP-013-1 Requirement R3** **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

Order No. 829 Citation	Directive / Guidance	Resolution
	that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	The directive is addressed in proposed CIP-013-1 Requirement R3 (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement R3:** Entities perform periodic assessment to keep plans up-to-date and, addressing current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC) *Implementation Guidance* developed by the drafting team and submitted for ERO endorsement includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and CIP-010-3 Requirements R1 Part 1.6. The 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. **Proposed CIP-010-3 Requirement R1** **R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*.

Order No. 829 Citation	Directive / Guidance	Resolution
		1.6. Prior to 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.
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5. The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach. **Proposed CIP-005-6 Requirement R2** **R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically

Order No. 829 Citation	Directive / Guidance	Resolution
		feasible, in CIP-005-6 Table R2 –Remote Access Management.: **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).
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by CIP-005-6 Requirement R2 Part 2.5 (above).
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address 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. 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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).
Objective 4: Vendor Risk Management and Procurement Controls		
P 59	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. Specifically, NERC must address controls for	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).

Order No. 829 Citation	Directive / Guidance	Resolution
	the following topics: (1) vendor security event notification processes; (2) vendor personnel termination 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. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	

Exhibit E

Implementation Guidance

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise-Endorsed Implementation Guidance.
Endorsement for this implementation guidance is based on the language of "draft 2" of the CIP-013-1 Reliability Standard dated April 2017. Any changes to the standard prior to the final ballot will require a reevaluation of the implementation guidance for continued endorsement.

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-1

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Reliability Standard **CIP-013-1 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1].

This implementation guidance provides considerations for implementing the requirements in CIP-013-1 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-1. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

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:*

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;*

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).*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security 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 terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is 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.

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.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security 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 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 the Responsible Entities 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.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-3, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

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:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". 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. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

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).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:

- Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
- Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

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;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

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;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

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*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

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

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

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

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.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

Requirement R3

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.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) “Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation”
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - “Cybersecurity Procurement Language for Energy Delivery Systems”

Exhibit F

Analysis of Violation Risk Factors and Violation Severity Levels

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-03 — Cyber Security — Supply Chain Risk Management

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **Project 2016-03 — Cyber Security — Supply Chain Risk Management.** Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines. The Cyber Security Supply Chain Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in an Operations Planning time horizon to develop one or more documented supply chain cyber security risk management plan(s). If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective, which is to develop one or more documented supply chain cyber security risk management plan(s). Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-013-1, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to develop one or more documented supply chain cyber security risk management plan(s) that set forth the controls.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in Operations Planning time horizon that requires entities to implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. If violated, failing to implement this plan could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) as specified in the requirement.

VSL Justifications for CIP-013-1, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R2 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSL is based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	R3 is a requirement in Operations Planning time horizon that requires the Responsible Entity to periodically review and obtain CIP Senior Manager or delegate approval of supply chain cyber security risk management plans. The reliability objective is to ensure plans remain up to date and address current and emerging supply chain-related cyber security concerns and vulnerabilities. If the requirement is violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R3 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of the review requirement by some number of months less than 18 calendar months does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-005-6, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in an Operations Planning and Same Day Operations time horizon to implement one or more documented processes for controlling vendor remote access to high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with the addition of two parts addressing specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-005-6, R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5)..	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

VSL Justifications for CIP-005-6, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	Theaddition of Parts 2.4 and 2.5 does not lower the current level of compliance.

the Current Level of Compliance	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R2 is not binary. Guideline 2b: The proposed VSLs do not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.

FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in Operations Planning time horizon that requires the Responsible Entity to implement one or more documented processes that include each of the applicable requirement parts for configuration change management. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with an additional part to address specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation

VSLs for CIP-010-3, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the	The Responsible Entity has not documented or implemented any configuration change management process(es) (R1); ; OR

required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1); . OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration (1.2); OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration (1.3); OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from

			the existing baseline configuration (1.4.1); OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change (1.4.2 & 1.4.3); OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration (1.5.1); OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and

			production environments (1.5.2); OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)

VSL Justifications for CIP-010-3, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The addition of Part 1.6 does not lower the currentl level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-010-3, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

Exhibit G

Summary of Development History and Complete Record of Development

Summary of Development History

Summary of Development History

The development record for proposed Reliability Standards CIP-005-6, CIP-010-3 and CIP-013-1 is summarized below.

I. Overview of the Standard Drafting Team

When evaluating a proposed Reliability Standard, the Commission is expected to give "due weight" to the technical expertise of the ERO.[1] The technical expertise of the ERO is derived from the standard drafting team selected to lead each project in accordance with Section 4.3 of the NERC Standards Process Manual.[2] For this project, the standard drafting team consisted of industry experts, all with a diverse set of experiences. A roster of the Standard Drafting team members is included in **Exhibit H**.

II. Standard Development History

A. Standard Authorization Request Development

Project 2016-03 – Cyber Security Supply Chain Risk Management was initiated on September 28, 2016 with the submission of a Standards Authorization Request ("SAR") to address the Commission's directives in Order No. 829.[3] In Order No. 829, the Commission direct[ed] NERC to develop a new or modified standard to address "supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."[4] Additionally, the Commission direct[ed] NERC to submit the new or modified Reliability Standard within one year of the effective date of Order No. 829. The SAR was posted for a 30-day informal comment period

---

1 Section 215(d)(2) of the Federal Power Act; 16 U.S.C. §824(d)(2) (2012).

2 The NERC *Standard Processes Manual* is available at http://www.nerc.com/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.pdf.

3 Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards* 154 FERC ¶ 61,050 (2016).

4 *Id.* at P 1.

from October 20, 2016 through November 18, 2016. The SAR was accepted by the Standards Committee on December 14, 2016.

B. First Posting - Comment Period, Initial Ballot and Non-binding Poll

Proposed Reliability Standard CIP-013-1, the associated Implementation Plan, Violation Risk Factors ("VRFs"), and Violation Severity Levels ("VSLs") were posted for a 45-day formal comment period from January 19, 2017 through March 6, 2017, with a parallel Initial Ballot and Non-binding Poll held during the last 10 days of the comment period from February 24, 2017 through March 6, 2017. The Initial Ballot for CIP-013-1 received 87.13% quorum, and 10.36% approval. The Non-binding Poll for the associated VRFs and VSLs received 82.34% quorum and 10.88% of supportive opinions. There were 134 sets of responses, including comments from approximately 231 different individuals and approximately 144 companies, representing all 10 industry segments.[5]

C. First and Second Postings - Comment Period, Initial/Additional Ballots and Non-binding Polls

NERC posted a second draft of CIP-013-1 and initial drafts of proposed Reliability Standards CIP-005-6 and CIP-010-3,[6] along with the associated Implementation Plan, VRFs, and VSLs for a 45-day formal comment period from May 2, 2017 through June 15, 2017, with parallel Initial Ballots for CIP-005-6 and CIP-010-3, an additional ballot for CIP-013-1 as well as the Non-binding Polls were held during the last 10 days of the comment period from June 6, 2017 through June 15, 2017.[7] The Initial Ballot for CIP-005-6 received 76.21% quorum, and

---

[5] NERC, *Consideration of Comments*, Project 2016-03 Cyber Security Supply Chain Risk Management (CIP-013-1), (May 2017), *available at* http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/2016-03_IB_Consideration%20of%20Comments_050217.pdf.

[6] The second posting for proposed Reliability Standard CIP-013-1 occurred simultaneously with the first posting for proposed Reliability Standards CIP-005-6 and CIP-010-3.

[7] The Non-binding Polls were extended an additional day reach quorum and closed June 16, 2017.

89.84% approval. The Initial Ballot for CIP-010-3 received 76.21% quorum, and 82.92% approval. The Additional Ballot for CIP-013-1 received 77.21% quorum, and 88.64% approval. The Non-binding Poll for CIP-005-6 received 76.15% quorum and 88.53% of supportive opinions. The Non-binding Poll for the CIP-010-3 received 76.29% quorum and 88.02% of supportive opinions. The related Non-binding Poll for CIP-010-3 received 76.35% quorum and 89.57% of supportive opinions. There were 101 sets of responses, including comments from approximately 220 different individuals and approximately 141 companies, representing all 10 industry segments.[8]

D. Final Ballot

Proposed Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1, were posted for a 10-final ballot period from July 11, 2017 through July 20, 2017. The ballot for proposed Reliability Standard CIP-005-6 and associated documents reached quorum at 81.59% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 88.79% of the voters. The ballot for proposed Reliability Standard CIP-010-3 and associated documents reached quorum at 81.33% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 81.40% of the voters. The ballot for proposed Reliability Standard CIP-013-1 and associated documents reached quorum at 82.84% of the ballot pool, and the standard received sufficient affirmative votes for approval, receiving support from 84.19% of the voters.

[8] NERC, *Consideration of Comments*, Project 2016-03 Cyber Security Supply Chain Risk Management, (July 11, 2017), *available at* http://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/2016-03_Consideration_of_Comments_07112017.pdf.

E. Board of Trustees Adoption

Proposed Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 were adopted by the NERC Board of Trustees on August 10, 2017.[9]

[9] NERC, *Board of Trustees Agenda Package*, Agenda Item 9a (CIP-013-1 – Cyber Security - Supply Chain Risk Management) *available at* http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Board_Open_Meeting_August_10_2017_Agenda_Package_v2%20(002).pdf.

Complete Record of Development

Project 2016-03 Cyber Security Supply Chain Risk Management

Related Files

Status
Final ballots concluded on **July 20, 2017** for the following standards:

- **CIP-005-6 - Cyber Security - Electronic Security Perimeter(s);**
- **CIP-010-3 - Cyber Security - Configuration Change Management and Vulnerability Assessments;** and
- **CIP-013-1 - Cyber Security - Supply Chain Risk Management**.

The voting results can be accessed via the links below. The standards will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Background
The project will address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 to develop a new or modified standard to address "supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations." *See* Order No. 829, at P 1.

Standard(s) Affected: The project will propose a new standard or revisions to approved Critical Infrastructure Protection (CIP) standards.

Purpose / Industry Need
On July 21, 2016 FERC issued Order No. 829, Revised Critical Infrastructure Protection Reliability Standards. In this order, FERC directed that NERC either develop a new standard or develop modifications to an existing standard to address the following reliability objective:

[FERC] directs] NERC to develop a 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, discussed in detail below: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls". *See* Order 829, at P 3.

The new standard or modified standard(s) are designed to "mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System" (*See* Order No. 829, at P 1) and must be filed with regulatory authorities within one year of the Order No 829 effective date.

Draft	Actions	Dates	Results	Consideration of Comments
Final Draft CIP-005-6 Clean **(43)** | Redline to Last Posted **(44)** | Redline to Last Approved **(45)** CIP-010-3	Final Ballot Info **(58)** Vote	07/11/17 – 07/20/17	Ballot Results CIP-005-6 **(59)** CIP-010-3 **(60)** CIP-013-1 **(61)**	

Clean **(46)** | Redline to Last Posted **(47)** | Redline to Last Approved **(48)** CIP-013-1 Clean **(49)**| Redline to Last Posted **(50)** Implementation Plan Clean **(51)** | Redline to Last Posted **(52)** **Supporting Materials** VRF/VSL Justification Clean **(53)** | Redline to Last Posted **(54)** Implementation Guidance **(55)** Consideration of Directives Clean **(56)** | Redline to Last Posted **(57)**				
Draft 1 CIP-005-6 Clean **(20)** | Redline **(21)** CIP-010-3 Clean **(22)** | Redline **(23)** **Draft 2** CIP-013-1 Clean **(24)** | Redline **(25)** Implementation Plan Clean **(26)** | Redline **(27)** **Supporting Materials** Unofficial Comment Form (Word) **(28)** VRF/VSL Justification Clean **(29)** | Redline **(30)** Implementation Guidance **(31)** Consideration of Directives Clean **(32)** | Redline **(33)** Draft RSAWs	Initial / Additional Ballots and Non-binding Polls Info **(34)** Vote	06/06/17 – 06/15/17 The non-binding polls were extended an additional day to reach quorum and closed June 16, 2017	Ballot Results CIP-005-6 **(35)** CIP-010-3 **(36)** CIP-013-1 **(37)** Non-binding Poll Results CIP-005-6 **(38)** CIP-010-3 **(39)** CIP-013-1 **(40)**	
	Comment Period Info **(41)** Submit Comments	05/02/17 – 06/15/17	Comments Received	Consideration of Comments **(42)**
	Join Ballot Pools	05/02/17 – 05/31/17		
	Info Send RSAW feedback to: RSAWfeedback@nerc.net	05/25/17 - 06/15/17		

<table>
<tr><td>CIP-005-6
Clean | Redline

CIP-010-3
Clean | Redline

CIP-013-1
Clean | Redline</td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="4">Draft 1

CIP-013-1 (8)

Implementation Plan (9)

Supporting Materials

Unofficial Comment Form (Word) (10)

VRF/VSL Justification (11)

Technical Guidance and Examples (12)

Consideration of Directives (13)

Draft Reliability Standard Audit Worksheet (RSAW)</td><td>Initial Ballot and Non-binding Poll

Info (14)

Vote</td><td>02/24/17 - 03/06/17</td><td>Ballot Results (15)

Non-binding Poll Results (16)</td><td></td></tr>
<tr><td>Comment Period

Info (17)

Submit Comments</td><td>01/19/17 - 03/06/17</td><td><><><><><><><><><
><><><><><><><>

Comments Received (18)</td><td>Consideration of Comments (19)</td></tr>
<tr><td>Join Ballot Pools</td><td>01/19/17 - 02/17/17</td><td></td><td></td></tr>
<tr><td>Info

Send RSAW feedback to: RSAWfeedback@nerc.net</td><td>02/03/17 - 03/06/17</td><td></td><td></td></tr>
<tr><td colspan="5">The Standards Committee accepted the Standards Authorization Request on December 14, 2016.</td></tr>
<tr><td>Standards Authorization Request (3)

Supporting Materials

Unofficial Comment Form (Word) (4)</td><td>Comment Period

Info (5)

Submit Comments</td><td>10/20/16 – 11/18/16</td><td>Comments Received (6)</td><td>Consideration of Comments (7)</td></tr>
<tr><td>Drafting Team Nominations

Supporting Materials

Unofficial Nomination Form (Word) (1)</td><td>Nomination Period

Info (2)

Submit Nominations</td><td>07/29/16 – 08/18/16</td><td></td><td></td></tr>
</table>

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Nomination Form

Project 2016-03 Cyber Security Supply Chain Management

Do not use this form for submitting nominations. Use the electronic form to submit nominations by **8 p.m. Eastern, Thursday, August 18, 2016.** This unofficial version is provided to assist nominees in compiling the information necessary to submit the electronic form.

Potential Standards Authorization Request and standards drafting team (SDT) members for Project 2016-03 Cyber Security Supply Chain Management should have significant management experience or subject matter expertise with the global supply system related to communications and control hardware, software, and services affecting BES operations and BES Cyber Systems. Expertise with developing and implementing controls, including policies, practices, guidelines, and standards designed to mitigate the introduction of cybersecurity risks in the supply chain is needed. In particular, drafting team experience is sought in areas associated with the four security objectives identified in Order No. 829, and potential nominees should highlight their experience in one or more of the objectives as part of their nomination:

(1) software integrity and authenticity;
(2) vendor remote access;
(3) information system planning; and
(4) vendor risk management and procurement controls.

Also, there is a need for a team member(s) with an understanding of the CIP Standards as discussed in Order No. 829 as well as procurement practices for BES Cyber Assets, with a focus on cyber security. In addition, compliance, legal, regulatory, facilitation, and technical writing skills are desired. Previous drafting team experience or other experience with development of standards is beneficial, but not required.

A significant time commitment is expected of SDT members to meet the one-year regulatory deadline established in Order No. 829. SDT activities include participation in technical conferences, stakeholder communications and outreach events, periodic drafting team meetings and conference calls. Approximately two in-person meetings per quarter can be expected (on average three full working days each meeting), as well as periodic conference calls as needed.

Additional information about this project is available on the Project 2016-03 Cyber Security Supply Chain Management page. If you have questions, contact Senior Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Name:	
Organization:	
Address:	
Telephone:	
E-mail:	

Please briefly describe your experience and qualifications to serve on the requested SDT (Bio). Highlight any experience in the four security objectives outlined in FERC Order No. 829 (1. software integrity and authenticity; 2. vendor remote access; 3. information system planning; and 4. vendor risk management and procurement controls):

If you are currently a member of any NERC drafting team, please list each team here:

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

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

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

☐ No prior NERC SAR or standard drafting team.

☐ Prior experience on the following team(s):

Select each NERC Region in which you have experience relevant to the Project for which you are volunteering:

☐ Texas RE	☐ NPCC	☐ SPP RE
☐ FRCC	☐ RF	☐ WECC
☐ MRO	☐ SERC	☐ NA – Not Applicable

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

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

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

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-03 Cyber Security Supply Chain Management

Drafting Team Nomination Period Open through August 18, 2016

Now Available

Nominations are being sought for members of the Project 2016-03 Standards Authorization Request and standard drafting team (SDT) through **8 p.m. Eastern, Thursday, August 18, 2016**.

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 that 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 Bulk Electric System (BES) operations as follows:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

The Commission also directed the new or revised Standard to be filed within one-year of the effective date of the Order.

Potential SDT members for Project 2016-03 Cyber Security Supply Chain Management should have significant management experience or subject matter expertise with the global supply system related to communications and control hardware, software, and services affecting BES operations and BES Cyber Systems. Expertise with developing and implementing controls, including policies, practices, guidelines, and standards designed to mitigate the introduction of cybersecurity risks in the supply chain is needed, with emphasis on experience in the four objectives outlined above. Also, there is a need for a team member(s) with an understanding of the CIP Standards as discussed in Order No. 829 as well as procurement practices for BES Cyber Assets, with a focus on cyber security. In addition, compliance, legal, regulatory, facilitation, and technical writing skills are desired. Previous drafting team experience or other experience with development of standards is beneficial, but not required.

A significant time commitment is expected of SDT members to meet the one-year regulatory deadline established in Order No. 829. SDT activities include participation in technical conferences,

stakeholder communications and outreach events, periodic drafting team meetings and conference calls. Approximately two in-person meetings per quarter can be expected (on average three full working days each meeting), as well as periodic conference calls as needed.

Use the electronic form to submit a nomination. If you experience any difficulties in using the electronic form, contact Nasheema Santos. An unofficial Word version of the nomination form is posted on the Standard Drafting Team Vacancies page and the project page.

Next Steps

NERC staff will present nominations to the Standards Committee in September 2016. Nominees will be notified shortly after the appointments have been made**.**

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

For more information or assistance, contact Senior Standards Developer, Mark Olson (via email) or at (404) 446-9760.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Cyber Security - Supply Chain Controls		
Date Submitted:	September 28, 2016		
SAR Requester Information			
Name:	Corey Sellers		
Organization:	Southern Company / Chair, SAR and Standards Drafting Team		
Telephone:	205-257-7531	E-mail:	mcseller@southernco.com
SAR Type (Check as many as applicable)			
☒ New Standard		☐ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the Standard action will achieve in support of Bulk Electric System reliability.):
The goal of this project is to establish forward-looking, objective-driven new or modified Reliability Standard(s) requiring entities to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and computing and networking services that impact Bulk Electric System (BES) operations. The project will address the Federal Energy Regulatory Commission (FERC) directives contained in Order No. 829.
Industry Need (What is the industry problem this request is trying to solve?):
On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven new or modified Reliability Standard(s) that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations. The supply chains for information and communications technology and industrial control systems present risks to the BES by providing potential opportunities for the introduction of

SAR Information
cybersecurity vulnerabilities. The new or modified Reliability Standard(s) is intended to reduce the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System.
Brief Description (Provide a paragraph that describes the scope of this Standard action.)
The Standards Drafting Team (SDT) shall develop new or modified Critical Infrastructure Protection (CIP) Standard(s) to require applicable entities to develop and implement a plan that includes security controls for supply chain management of industrial control system hardware, software, and computing and networking services that impact BES operations as described in Order No. 829. The work will include development of an Implementation Plan, Violation Risk Factors, Violation Severity Levels, and supporting documents, within the 12-month deadline established by FERC in Order No. 829.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the Standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the Standard action.)
The SDT shall address each of the Order No. 829 directives. The Reliability Standard(s) developed or revised in the project will require applicable entities to develop and implement a plan that addresses, at a minimum, the following four specific objectives as they relate to supply chain cybersecurity of the BES (Order No. 829 at P 45): 1. Software integrity and authenticity; 2. Vendor remote access; 3. Information system planning; and 4. Vendor risk management and procurement controls. The plan may apply different controls based on the criticality of different assets (Order No. 829 at P 44). Requirements developed by the SDT will be aimed at the protection of aspects of the supply chain that are within the control of responsible entities (Order No. 829 at P 10). The new or modified Reliability Standard will also require periodic reassessment of the applicable entity's selected controls by the applicable entity's CIP Senior Manager at least every 15 months (Order No. 829 at P 46). In addressing Objective 1 (Software integrity and authenticity), the SDT shall develop requirement(s) for applicable entities to 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. (Order No. 829 at P 48) In addressing Objective 2 (Vendor remote access), the SDT shall develop requirement(s) for applicable entities to address logging and controlling all third-party (i.e., vendor) initiated remote access sessions. The objective covers both user-initiated and machine-to-machine vendor remote access. Additionally,

SAR Information
applicable entities' controls must provide for rapidly disabling remote access sessions to mitigate a security event, if necessary. (Order No. 829 at P 51 and 52) In addressing Objective 3 (Information system planning), the SDT shall develop requirement(s) that address the applicable entities' CIP Senior Manager (or delegate) identification and documentation of risks for consideration by the applicable entity in proposed information system planning. (Order No. 829 at P 56) In addressing Objective 4 (Vendor risk management and procurement controls), the SDT shall develop requirement(s) for applicable entities to address the provision and verification of the following security concepts, at a minimum, in future contracts for industrial control system hardware, software, and computing and networking services associated with BES operations. (Order No. 829 at P 59) • Vendor security event notification processes; • Vendor personnel termination notification for employees with access to remote and onsite systems; • Product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; • Coordinated incident response activities; and • Other related aspects of procurement that the SDT determines should be addressed for supply chain cyber security risk management as stated in Order No. 829. The SDT may, as an alternative, propose an equally efficient and effective means to meet the objectives in Order No. 829.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.

Reliability Functions		
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.

Reliability and Market Interface Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

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

Related Standards	
Standard No.	Explanation
CIP-002-5	Cyber Security - BES Cyber System Categorization. Specifies categorization of BES Cyber Systems and BES Cyber Assets to support appropriate protection against compromises that could lead to misoperation or instability in the BES.
CIP-003-6	Cyber Security - Security Management Controls. Establishes responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in BES
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-007-6	Cyber Security - System Security Management

Related Standards	
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on the Standards Authorization Request (SAR) developed by NERC Staff. The electronic comment form must be completed by **8:00 p.m. Eastern, Friday, November 18, 2016**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 that 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 Bulk Electric System (BES) operations as follows:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

The Commission also directed the new or revised Standard to be filed within one-year of the effective date of the Order.

The drafting team has developed a SAR for new or modified Critical Infrastructure Protection (CIP) Standard(s) to require applicable entities to develop and implement plan(s) that include security controls for supply chain management of industrial control system hardware, software, and computing and networking services that impact BES operations as described in Order No. 829.

Questions

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

1. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.
Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-03 Cyber Security Supply Chain Management Standards Authorization Request

Informal Comment Period Open through November 18, 2016

Now Available

A 30-day informal comment period for the **Project 2016-03 Cyber Security Supply Chain Management** Standards Authorization Request (SAR), is open through **8 p.m. Eastern, Friday, November 18, 2016**.

Commenting

Use the electronic form to submit comments on the SAR. If you experience any difficulties using the electronic form, contact Nasheema Santos. An unofficial Word version of the comment form is posted on the project page.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 8 p.m. Eastern).

Next Steps

The drafting team will review all responses received during the comment period and determine the next steps of the project.

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

For more information or assistance, contact Senior Standards Developer, Mark Olson (via email) or at (404) 446-9760.

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

Comment Report

Project Name:	2016-03 Cyber Security Supply Chain Management | SAR October 2016
Comment Period Start Date:	10/20/2016
Comment Period End Date:	11/18/2016
Associated Ballots:	

There were 24 sets of responses, including comments from approximately 24 different people from approximately 23 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
ACES Power Marketing	Ben Engelby	6		ACES Standards Collaborators - CIP	Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Ginger Mercier	Prairie Power, Inc.	3	SERC
					Tara Lightner	Sunflower Electric Power Corporation	1	SPP RE
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Bill Watson	Old Dominion Electric Cooperative	3,4	RF
					Cassie Williams	Golden Spread Electric Cooperative	3,5	SPP RE
					Scott Brame	North Carolina Electric Membership Corporation	3,4,5	SERC
					Ryan Strom	Buckeye Power, Inc.	3,4,5	RF
					Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
					Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC
					Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
					Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3	SPP RE
					Kevin Lyons	Central Iowa	1	MRO

						Power Cooperative		
					Carl Behnke	Southern Maryland Electric Cooperative	3	RF
					Susan Sosbe	Wabash Valley Power Association	3	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	3,4,5,6	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Lower Colorado River Authority	Michael Shaw	1,5,6		LCRA Compliance	Teresa Cantwell	LCRA	1	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC

Wayne Sipperly	New York Power Authority	4	NPCC
David Ramkalawan	Ontario Power Generation	4	NPCC
Glen Smith	Entergy Services	4	NPCC
Brian Robinson	Utility Services	5	NPCC
Bruce Metruck	New York Power Authority	6	NPCC
Alan Adamson	New York State Reliability Council	7	NPCC
Edward Bedder	Orange & Rockland Utilities	1	NPCC
David Burke	UI	3	NPCC
Michele Tondalo	UI	1	NPCC
Sylvain Clermont	Hydro Quebec	1	NPCC
Si Truc Phan	Hydro Quebec	2	NPCC
Helen Lainis	IESO	2	NPCC
Laura Mcleod	NB Power	1	NPCC
MIchael Forte	Con Edison	1	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Kelly Silver	Con Edison	3	NPCC
Peter Yost	Con Edison	4	NPCC
Brian O'Boyle	Con Edison	5	NPCC
Greg Campoli	NY-ISO	2	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
Sean Bodkin	Dominion	4	NPCC
Michael Schiavone	National Grid	1	NPCC
Michael Jones	National Grid	3	NPCC

Lower Colorado River Authority	Teresa Cantwell	1,5,6		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Midcontinent ISO, Inc.	Terry BIlke	2		IRC-SRC	Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

Thomas Foltz - AEP - 3,5

Answer	No
Document Name	

Comment

AEP has two comments to offer. First, AEP suggests a broader approach to the drafting team's efforts to achieve the directive set forth by FERC. The specificity of the SAR leaves little room for debate and interpretation, as evidenced by the first draft of the standard. Specifically, AEP encourages the drafting team to allow for flexibility based on size of entity and size of vendor as well as the impact category and other attributes of the affected BES Cyber System(s). The SAR could include a statement that there are specific security vulnerabilities or controls to be addressed in a procurement or supply chain process. This may better focus the drafting team on implementing the most effective standard possible.

Second, AEP recognizes the need to move quickly, but holding a technical conference on the first draft of the standard seems premature when the SAR is not yet agreed upon.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC

Answer	No
Document Name	

Comment

We have suggestions on

1) Purpose,

2) Industry Need,

3) Brief Description

4) Detailed Description to better define this project's scope.

For Purpose, we have three recommendations

A) change "supply chain management" to "supply chain risk management";

B) change “and implement a plan that includes security controls for supply chain management for” to “and implement measures for supply chain risk management for”;

C) copy the final industry need sentence to the Purpose – “The new or modified Reliability Standard(s) is intended to reduce the risk of a cyber security incident affecting the reliable operation of the Bulk-Electric System.”

Supply chain management is the flow of goods, services and resources that involve the movement, storage and maintenance of material for work in progress. Supply chain risk management is a subset of supply chain management. For this SAR, supply chain risk management should focus on the risks associated with sourcing and servicing BES Cyber System Components from external entities.

For Industry Need, we have one recommendation – change “On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven new or modified Reliability Standard(s) that addresses” to “On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven, risk-based new or modified Reliability Standard(s) that addresses”

For Brief Description, we have one recommendation – update the Brief Description to be consistent with our proposed changes to the Purpose and Industry Need.

For Detailed Description, we have one recommendation – change “The plan may apply different controls based on the criticality of different assets (Order No. 829 at P44)” to “The plan may apply different measures based on the criticality of different assets (Order No. 829 at P44)”

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

The technical guidelines may imply stricter requirements versus providing guidance.

This has the potential to expand the scope for Low Impact BCS which impacts compliance resources. NRG strongly recommends to the SDT that they consider impact rating criteria first, and then factor in a risk based approach. NRG recommends that the SAR states correctly that the draft is a Supply Chain Risk Management Standard.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5 - WECC

Answer	No
Document Name	

Comment

Due to the possible complexity of creating a workable new standard, Reclamation recommends that a pilot program be developed to invite any entity to volunteer to test and implement a draft of the standard prior to it being finalized. During the pilot program, vendors are also invited to participate in order to work out any verification processes of the standard. Once the standard is finalized, the enforcement of the standard should apply to facilities that are rated as high impact facilities on the first year, facilities that are rated as medium impact on the second year, and facilities that are rated as low impact on the third year.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6

Answer	No
Document Name	

Comment

The project "**2016-03 Cyber Security Supply Chain Management "–** The four objectives listed under this new CIP standard can be better served by providing some updates in the current CIP Standards. Specifically, Objective 2 below, is already included in the current standard for CIP-005-5 R2 Interactive Remote Access Management for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity. This objective can be better served by providing updates to the CIP-005-5 Requirement R2.

Objective 3 is already provided at LADWP by its best practices processes of requiring any IT related purchases to go through a review and approval process by our Information Technology Systems Division. This objective can be better served through an update to the current CIP-003-6 Standard.

In summary, the Objectives of the Cyber Security Supply Chain Management can be efficiently and effectively implemented through updates on the current Version 5 and Version 6 CIP Standards.

Cyber Security Supply Chain Management Objectives:

1. Software integrity and authenticity;
2. Vendor remote access;
3. Information system planning; and
4. Vendor risk management and procurement controls.

Likes 0	
Dislikes 0	

Response

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison

Answer	Yes
Document Name	

Comment
Answer above should be No. System not allowing me to change it. Con Edison Company of New York supports NPCC RSC's comments on this SAR.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	

Comment
Duke Energy agrees with the scope of the project, in that the scope of the project appears to stem directly from FERC Order 829. We agree with the SAR wherein the designation is made that there is a possibility that revisions to CIP standards may be a solution, and not just the creation of a new standard.

Likes 0	
Dislikes 0	

Response

Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	Yes
Document Name	

Comment
Seminole supports the work of this team and the proposed SAR. Seminole further suggests that the SAR specifically address BES Cyber Security Information stored at vendor locations. As cloud information storage is the predominate trend, clarity of requirements for vendors related to both storage of information provided to vendors and vendor responsibilities for information stored in the cloud should be addressed at least in the Guidelines and Technical Basis.

Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance

Answer	Yes
Document Name	
Comment	

Objective 1- “Integrity of software and patches” Comment for Internal LCRA -There are lot of whitepapers on Software Integrity Levels(SIL) . We might need to come up with Software Integrity levels for each control system and develop contractual language with the respective vendor to accept that Level and the associated responsibilities/SLAs. We will need to work with Purchasing to develop the new language

Objective 3 – Comment for SAR- on Information system planning- What is Information system planning?. Not well understood. The SAR information does not adequately that describe beyond entities needing to document the risks we take into consideration. Would like to see additional description on Information System Planning

Likes 0	
Dislikes 0	
Response	

Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Yes, we agree with the scope. However, we would like consideration given to the following:
Idaho Power believes that tightening purchasing controls too tightly could also pose a risk because there are limited vendors that service its needs. The vendors that derive a large portion of their business from the electric industry would likely be willing to adapt to such new requirements. Providers that have a larger customer base may not be as willing to adjust to practices to meet any new requirements. Due to this concern, Idaho Power believes that the supply chain standard should be laid out in terms of requirements built around controls that are developed by the regulated entity rather than perspective requirements like many other CIP standards. Such flexibility would provide a foundation for the standard to evolve.
Idaho Power believes that such a significant undertaking will take years to develop and implement. Idaho Power believes that such a proposal will need to clearly define the requirements of what materials should be impacted. It would also need to set forth the types of documentation that could be used to verify that requirements are met. Idaho Power and other entities would then need time to add language to its contracts to ensure compliance by its suppliers and any sub-suppliers. Idaho Power believes that such a process would require significant time, money, and resources and would result in higher costs for materials, which would impact Idaho Power's customers. Idaho Power believes it would be valuable for NERC to look into whether other regulatory agencies or industries have addressed such a requirement as a starting point for such reliability standards.

Likes 0	
Dislikes 0	
Response	

Linsey Ray - Oncor Electric Delivery - NA - Not Applicable - Texas RE	
Answer	Yes
Document Name	

Comment

Title of Proposed Standard(s): Cyber Security – Supply Chain Risk Management

Oncor recommends changing the title to more closely reflect the FERC directive. The intent is to manage risk associated with the supply chain. Calling out controls in the title could be interpreted as adding specific controls to the process and not fully evaluating the risks associated with the supply chain process. This is also called out in paragraph 1 of the order "… develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware…".

In addressing Objective 3 (Information system planning), the SDT shall develop requirement(s) that address the applicable entities' CIP Senior Manager (or delegate) identification and documentation of security risks for consideration by the applicable entity in proposed information system planning. (Order No. 829 at P 56)

Oncor recommends adding the word "security" to this statement. If taken out of context, the standard could be seen as opening it up to all risks associated with information system planning. This interpretation could be expanded greatly beyond the original intent of improving reliability through a secure Information Technology system. Examples of risks that should be considered 'out of scope' would include product delivery timing and special packaging requirements. While paragraph 56 doesn't specifically call out security, the intent of Order 829 clearly focuses on ensuring the security of key BES cyber systems and components.

In addressing Objective 4 (Vendor risk management and procurement controls), the SDT shall develop requirement(s) for applicable entities to address the provision and verification of the following security concepts, at a minimum, in future contracts for industrial control system hardware, software, and computing and networking services associated with BES operations. (Order No. 829 at P 59)

Oncor recommends removing the phrase "at a minimum" from this section. The phrase could encourage an audit team to expect or request more evidence than intended by this objective. This phrase is not mentioned in paragraph 59; "verification of relevant security concepts_in future contracts for industrial control system hardware,".

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes
Document Name	

Comment

Occidental Chemical Corporation agrees with the proposed scope of Project 2016-03 as described in the SAR but offers the following suggestions:

- Purpose section of SAR states that the project will cover "security controls for supply chain management" but should probably be revised to state that it will cover "security controls for supply chain *risk* management" to be consistent with FERC Order 829 and the Industry Need section of the SAR.
- Purpose section of SAR states that the new or modified Reliability Standard(s) will require entities to "develop and implement a plan" – the SAR shouldn't assume that the agreed upon approach will be a "plan" and should be revised to read "develop and implement measures". This will allow the SDT the most flexibility if it is later determined that a "plan" is not the best approach and will still allow for a "plan" if the entity determines that to be the best approach

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	Yes
Document Name	

Comment

Thank you for this opportunity to provide comments on the Standards Authorization Request (SAR) written in response to Order No. 829 that will direct the development of a new or modified Reliability Standard for supply chain risk management to industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations. While FERC clearly wants to advance the state of supply chain security, we believe the inclusion of Low Impact Cyber Assets will delay the SDT's ability to make the one year filing deadline. We believe the SAR should narrow its focus to the 'highest watermark' first, to limit confusion, especially as entities prepare for implementing activities that address the Low Impact aspects of their programs. Other SDTs continue to enhance related NERC CIP standards based on changes to the definitions for Low Impact External Routable Connectivity and Transient Cyber Assets.

All security advances and efficiencies designed for large-sized utilities, including their choice of software and hardware vendors, will eventually pass down to the Medium Impact Facilities, and ultimately to the Low Impact Facilities, through better IT security testing and best practices. This natural progression takes time and maturity to nurture, something we feel should be allowed reflected within in the SAR.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance

Answer	Yes
Document Name	

Comment

Objective 3 – Regarding Information System Planning - What is Information System Planning? It is not well understood. The SAR information does not adequately describe that beyond entities needing to document the risks we take into consideration. We would like to see additional description on Information System Planning.

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Document Name	
Comment	
PJM agrees with the language within the Project 2016-03 Cyber Security Supply Chain Management SAR and asks the SDT to consider the following comments when developing the standard. As stated within paragraph 42 of the order, PJM agrees with the APPA that the standard should be risk based as opposed to impact based. PJM also asks the SDT to consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within addressing the four objectives outlined in the order or by adding an additional objective.	
Likes 0	
Dislikes 0	
Response	
Sophia Combs - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Coon - Open Access Technology International, Inc. - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Document Name	
Comment	
The IRC members ask the Standard Drafting Team (SDT) to consider the following comments when developing the standard. As stated within paragraph 42 of the order, the IRC members agree with the APPA that the standard should be risk based as opposed to impact based. The IRC members also ask the SDT to consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within the four objectives outlined in the order or by adding an additional objective.	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	
Document Name	
Comment	
Reclamation recommends that the CIP language be written to account for existing Government procurement constraints; or exempt the government entities that are legally bound by federal procurement regulations.	
Likes 0	
Dislikes 0	

Response
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF
Answer	
Document Name	
Comment
N/A
Likes 0	
Dislikes 0	
Response
Michelle Coon - Open Access Technology International, Inc. - NA - Not Applicable - NA - Not Applicable
Answer	
Document Name	
Comment
Open Access Technology international, Inc. (OATI) appreciates this opportunity to submit comments pertaining to the Cyber Security Supply Chain Management Standards Authorization Request (SAR). Tackling such a large and important issue is no easy feat. Yet, the standard drafting team has already demonstrated their commitment to this difficult and important task by creating a new draft standard for the most recent technical conference. Continued dedication to this effort will help ensure the new reliability standard is consistent and equally applicable to necessary areas of the bulk electric system. As a committed provider of software solutions and services to the electric utility sector, OATI plans to participate in the standard drafting process to the fullest extent possible. There are significant challenges ahead that can benefit from OATI's perspective into all of the various aspects of the electric utility reliability. OATI has identified two significant challenges: consistency in application and manageability. OATI observes a need to develop a consistent approach to applying this standard across the industry, large and small vendors, niche and cross-sector vendors. This will include taking into consideration the fact that some vendors which also focus heavily in other industries, may be less willing to accommodate a utility's need to meet this new NERC reliability standard. Smaller utilities, especially, could be presented with a "take it or leave it" proposition from vendors such as Microsoft, CISCO, or Dell. Additionally, there is a special issue presented by the widespread use of open source software in many software solutions today. A standard should not apply only to one subset of vendors/software. Rather, to avoid a discriminatory impact, the standard should be equally applicable to all in-scope vendors/ software solutions. While this issue of consistency presents many challenges, OATI stands eager to share ideas for reaching a reasonable resolution. Another related challenge is one of manageability. To facilitate a manageable approach, OATI observes a need for NERC to establish a common baseline standard applicable to all in scope vendors/software. This should help avoid issues on both sides of the supply chain. Absent a baseline, utilities may each develop a variety of inconsistent approaches to meeting the objectives of the standard. Such inconsistency is likely to create major problems for vendors as they verify compliance with the standard. The downstream impact of such inconsistent approaches is an increased burden on vendors who may each develop a unique way to meet the objectives passed onto them. Fortunately, much work has already been completed by the Department of Energy and the National Institute of Standards and Technology in this area of supply chain security that will be helpful in defining the baseline for this industry. These existing approaches should be considered and leveraged in the development of this new CIP supply chain

management standard.

OATI looks forward to working closely with NERC, industry members, and other vendors in shaping this new reliability standard. A special thanks to NERC for its inclusion of the vendors in this important and necessary effort. Together we can successfully develop a consistent and manageable standard to mitigate this cybersecurity vulnerability in the bulk electric system.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC

Answer	
Document Name	

Comment

We also recommend that the SDT seriously consider updating existing CIP Standards in order to avoid creating double jeopardy for

A) remote access (CIP-005 R2);

B) patch management (CIP-007 R2);

C) authentication (CIP-007 R5);

D) vendor termination of employees (CIP-004 R5);

We recommend that new Requirements do not jeopardize existing Requirements and their implementation timelines, and that new Requirements do not create additional paperwork with little value to the Reliable Operation of the Bulk Electric System.

Likes 0	
Dislikes 0	

Response

Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP

Answer	
Document Name	

Comment

If the SDT proposes to modify Low Impact requirements, we recommend maintaining them in Attachment 1 of NERC Standard CIP-003-6. Additions to Section 3: Access Controls could be made for future patch management requirements. We believe Section 4: Cyber Security Incident Response could be modified to include vendor remote termination access within a specified timeframe. The new definition of Transient Cyber Device could also be used as the location for baseline configuration management.

We believe all Low Impact processes should be non-prescriptive and provide flexibility for registered entities to decide how to best defend against cyber

security threats based on their risk analysis. There may be significant advantages and protection for industry to adopt new supply chain requirements for those entities that have multiple vendors and large support staff. We believe that BES risks and economies of scale for G&T cooperatives are minimal, based on their size and geographical location within the BES.

Thank you for your time and attention regarding this SAR.

Likes 0	
Dislikes 0	

Response

Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF

Answer	
Document Name	

Comment

ITC Holdings finds this new standard to be ovrely burdensome for smaller utilities that do not have the infrastructure or staffing to perform the activities.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	
Document Name	

Comment

The IESO suggests the Standard Drafting Team (SDT) consider the following comments when developing the standard. As stated within paragraph 42 of the order, the IESO agrees that the standard should be risk based as opposed to impact based. The IESO also suggests the SDT consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within the four objectives outlined in the order or by adding an additional objective.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 3,5

Answer	
Document Name	

Comment
AEP suggests that any supply chain cyber security requirements applicable to low impact BES Cyber Systems be written in a revised CIP-003, Requirement R2, Attachment 1.

Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance

Answer	
Document Name	

Comment
None

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	
Document Name	

Comment
We would like to point out the potential need for future modifications on other CIP standards as a result of this project. Specifically, there may be some language conflicts that arise, or duplicative controls put in place. Also, some ability will need to be afforded to entities allowing for the capability of verifying with a vendor, the integrity and authenticity of its software. Next, we feel like the language in the SAR should be revised to reflect a concentration on security controls for supply chain *risk* management, rather than just security controls for supply chain management. We feel the added emphasis on risk is appropriate in this context. Lastly, we want to point out to the drafting team the importance of keeping separate the topics of operations versus supply chain. We can see where instances may occur wherein the language of a standard can be intended to focus on supply chain aspects, but to the reader, may bleed over into the operations space.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
This SAR, if approved, allows the Standards Drafting Team (SDT) to develop new or modified Critical Infrastructure Protection (CIP) Standard(s) for supply chain management to address the Federal Energy Regulatory Commission (FERC) directives contained in Order No. 829. Texas RE supports developing new CIP Standard(s) to address supply chain management, which should be applicable to high, medium, and low impact BES Cyber Systems. Modifying existing CIP Standard(s) has caused confusion in the industry in regard to implementation dates. For example, CIP-003-6, added low impact Requirements, with multiple implementation dates.	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name: 2016-03 Cyber Security Supply Chain Management | SAR October 2016

Comment Period Start Date: 10/20/2016

Comment Period End Date: 11/18/2016

Associated Ballots:

There were 24 sets of responses, including comments from approximately 24 different people from approximately 23 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
ACES Power Marketing	Ben Engelby	6		ACES Standards Collaborators - CIP	Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Ginger Mercier	Prairie Power, Inc.	3	SERC
					Tara Lightner	Sunflower Electric Power Corporation	1	SPP RE
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Bill Watson	Old Dominion Electric Cooperative	3,4	RF
					Cassie Williams	Golden Spread Electric Cooperative	3,5	SPP RE
					Scott Brame	North Carolina Electric	3,4,5	SERC

	Membership Corporation		
Ryan Strom	Buckeye Power, Inc.	3,4,5	RF
Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC
Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3	SPP RE
Kevin Lyons	Central Iowa Power Cooperative	1	MRO
Carl Behnke	Southern Maryland	3	RF

						Electric Cooperative		
					Susan Sosbe	Wabash Valley Power Association	3	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	3,4,5,6	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Lower Colorado River Authority	Michael Shaw	1,5,6		LCRA Compliance	Teresa Cantwell	LCRA	1	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC

					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC

Bruce Metruck	New York Power Authority	6	NPCC
Alan Adamson	New York State Reliability Council	7	NPCC
Edward Bedder	Orange & Rockland Utilities	1	NPCC
David Burke	UI	3	NPCC
Michele Tondalo	UI	1	NPCC
Sylvain Clermont	Hydro Quebec	1	NPCC
Si Truc Phan	Hydro Quebec	2	NPCC
Helen Lainis	IESO	2	NPCC
Laura Mcleod	NB Power	1	NPCC
MIchael Forte	Con Edison	1	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Kelly Silver	Con Edison	3	NPCC
Peter Yost	Con Edison	4	NPCC
Brian O'Boyle	Con Edison	5	NPCC
Greg Campoli	NY-ISO	2	NPCC

					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Lower Colorado River Authority	Teresa Cantwell	1,5,6		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Midcontinent ISO, Inc.	Terry BIlke	2		IRC-SRC	Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.	
Thomas Foltz - AEP - 3,5	
Answer	No
Comment	
AEP has two comments to offer. First, AEP suggests a broader approach to the drafting team's efforts to achieve the directive set forth by FERC. The specificity of the SAR leaves little room for debate and interpretation, as evidenced by the first draft of the standard. Specifically, AEP encourages the drafting team to allow for flexibility based on size of entity and size of vendor as well as the impact category and other attributes of the affected BES Cyber System(s). The SAR could include a statement that there are specific security vulnerabilities or controls to be addressed in a procurement or supply chain process. This may better focus the drafting team on implementing the most effective standard possible. Second, AEP recognizes the need to move quickly, but holding a technical conference on the first draft of the standard seems premature when the SAR is not yet agreed upon.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will consider your suggestions for allowing flexibility based on entity and vendor factors and asset impact category during standards development. The SAR provides the SDT with this flexibility as written. NERC determined that a technical conference could be beneficial to the SDT and industry by providing an early opportunity to discuss initial draft requirements and considerations for addressing the directives in Order No. 829. The approach has been used successfully in other projects with time-sensitive directives.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No

Comment
We have suggestions on 1) Purpose, 2) Industry Need, 3) Brief Description 4) Detailed Description to better define this project's scope.   For Purpose, we have three recommendations A) change "supply chain management" to "supply chain risk management"; B) change "and implement a plan that includes security controls for supply chain management for" to "and implement measures for supply chain risk management for"; C) copy the final industry need sentence to the Purpose – "The new or modified Reliability Standard(s) is intended to reduce the risk of a cyber security incident affecting the reliable operation of the Bulk-Electric System." Supply chain management is the flow of goods, services and resources that involve the movement, storage and maintenance of material for work in progress. Supply chain risk management is a subset of supply chain management. For this SAR, supply chain risk management should focus on the risks associated with sourcing and servicing BES Cyber System Components from external entities. For Industry Need, we have one recommendation – change "On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven new or modified Reliability Standard(s) that addresses" to "On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven, risk-based new or modified Reliability Standard(s) that addresses"

For Brief Description, we have one recommendation – update the Brief Description to be consistent with our proposed changes to the Purpose and Industry Need. For Detailed Description, we have one recommendation – change “The plan may apply different controls based on the criticality of different assets (Order No. 829 at P44)” to “The plan may apply different measures based on the criticality of different assets (Order No. 829 at P44)”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that the purpose of the project is to develop requirements that address supply chain *risk* management and has revised the SAR Purpose section and Brief Description section accordingly. The SDT does not believe the other suggested changes to the purpose section improve clarity or change the project scope. The purpose states that entities will be required to *develop and implement a plan*, which aligns with Order No. 829 directives (P 43 and 45). The SAR provides for the development of an equally effective and efficient alternative, which could include requirements for implementing measures instead of a plan. The SAR provides latitude to develop risk-based standard(s) as written. The suggested revision is not being incorporated in the SAR because it could be incorrectly attributed to FERC. The SDT does not believe the suggested change in the detailed description from 'controls' to 'measures' changes the project scope or provides additional clarity. Accordingly, the SDT is maintaining wording to align with Order No 829 P 44.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Comment	
The technical guidelines may imply stricter requirements versus providing guidance.	

This has the potential to expand the scope for Low Impact BCS which impacts compliance resources. NRG strongly recommends to the SDT that they consider impact rating criteria first, and then factor in a risk based approach. NRG recommends that the SAR states correctly that the draft is a Supply Chain Risk Management Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has incorporated 'Risk Management' wording throughout the SAR. NRG's comments will be considered during standards development.	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Comment	
Due to the possible complexity of creating a workable new standard, Reclamation recommends that a pilot program be developed to invite any entity to volunteer to test and implement a draft of the standard prior to it being finalized. During the pilot program, vendors are also invited to participate in order to work out any verification processes of the standard. Once the standard is finalized, the enforcement of the standard should apply to facilities that are rated as high impact facilities on the first year, facilities that are rated as medium impact on the second year, and facilities that are rated as low impact on the third year.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is developing requirements to address FERC directives contained in Order No. 829 and must file new or modified standard(s) within 12 months. The SDT will not use a pilot program, but will resolve stakeholder issues using the standards development process. The SDT will consider U.S. Bureau of Reclamation's suggestions for implementation during standards development.	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	

Answer	No
Comment	

The project "**2016-03 Cyber Security Supply Chain Management "–** The four objectives listed under this new CIP standard can be better served by providing some updates in the current CIP Standards. Specifically, Objective 2 below, is already included in the current standard for CIP-005-5 R2 Interactive Remote Access Management for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity. This objective can be better served by providing updates to the CIP-005-5 Requirement R2.

Objective 3 is already provided at LADWP by its best practices processes of requiring any IT related purchases to go through a review and approval process by our Information Technology Systems Division. This objective can be better served through an update to the current CIP-003-6 Standard.

In summary, the Objectives of the Cyber Security Supply Chain Management can be efficiently and effectively implemented through updates on the current Version 5 and Version 6 CIP Standards.

Cyber Security Supply Chain Management Objectives:

1. Software integrity and authenticity;
2. Vendor remote access;
3. Information system planning; and
4. Vendor risk management and procurement controls.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT is considering both development of new standards, and revisions to existing standards, in determining how to address the directives in Order No. 829.

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison	
Answer	Yes
Comment	
Answer above should be No. System not allowing me to change it. Con Edison Company of New York supports NPCC RSC's comments on this SAR.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT notes that Con Ed does not support the SAR. See response to NPCC above.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Comment	
Duke Energy agrees with the scope of the project, in that the scope of the project appears to stem directly from FERC Order 829. We agree with the SAR wherein the designation is made that there is a possibility that revisions to CIP standards may be a solution, and not just the creation of a new standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes

Comment	
Seminole supports the work of this team and the proposed SAR. Seminole further suggests that the SAR specifically address BES Cyber Security Information stored at vendor locations. As cloud information storage is the predominate trend, clarity of requirements for vendors related to both storage of information provided to vendors and vendor responsibilities for information stored in the cloud should be addressed at least in the Guidelines and Technical Basis.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will consider Seminole Electric Cooperative's comment during standards development.	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Comment	
Yes, we agree with the scope. However, we would like consideration given to the following: Idaho Power believes that tightening purchasing controls too tightly could also pose a risk because there are limited vendors that service its needs. The vendors that derive a large portion of their business from the electric industry would likely be willing to adapt to such new requirements. Providers that have a larger customer base may not be as willing to adjust to practices to meet any new requirements. Due to this concern, Idaho Power believes that the supply chain standard should be laid out in terms of requirements built around controls that are developed by the regulated entity rather than perspective requirements like many other CIP standards. Such flexibility would provide a foundation for the standard to evolve. Idaho Power believes that such a significant undertaking will take years to develop and implement. Idaho Power believes that such a proposal will need to clearly define the requirements of what materials should be impacted. It would also need to set forth the types of documentation that could be used to verify that requirements are met. Idaho Power and other entities would then need time to add language to its contracts to ensure compliance by its suppliers and any sub-suppliers. Idaho Power believes that such a process would require significant time, money, and resources and would result in higher costs for materials, which would impact Idaho Power's customers. Idaho Power believes it would be	

valuable for NERC to look into whether other regulatory agencies or industries have addressed such a requirement as a starting point for such reliability standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider them during standards development. The SDT agrees that the standard should provide flexibility for entities to determine approaches to meet the reliability objectives contained in Order No. 829. The SDT is considering guidance and reference material that includes input from government and other regulated sectors, including references cited in Order No. 829.	
Linsey Ray - Oncor Electric Delivery - NA - Not Applicable - Texas RE	
Answer	Yes
Comment	

Title of Proposed Standard(s): Cyber Security – Supply Chain Risk Management

Oncor recommends changing the title to more closely reflect the FERC directive. The intent is to manage risk associated with the supply chain. Calling out controls in the title could be interpreted as adding specific controls to the process and not fully evaluating the risks associated with the supply chain process. This is also called out in paragraph 1 of the order "… develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware…".

In addressing Objective 3 (Information system planning), the SDT shall develop requirement(s) that address the applicable entities' CIP Senior Manager (or delegate) identification and documentation of security risks for consideration by the applicable entity in proposed information system planning. (Order No. 829 at P 56)

Oncor recommends adding the word "security" to this statement. If taken out of context, the standard could be seen as opening it up to all risks associated with information system planning. This interpretation could be expanded greatly beyond the original intent of improving reliability through a secure Information Technology system. Examples of risks that should be considered 'out of scope' would include product

delivery timing and special packaging requirements. While paragraph 56 doesn't specifically call out security, the intent of Order 829 clearly focuses on ensuring the security of key BES cyber systems and components.

In addressing Objective 4 (Vendor risk management and procurement controls), the SDT shall develop requirement(s) for applicable entities to address the provision and verification of the following security concepts, at a minimum, in future contracts for industrial control system hardware, software, and computing and networking services associated with BES operations. (Order No. 829 at P 59)

Oncor recommends removing the phrase "at a minimum" from this section. The phrase could encourage an audit team to expect or request more evidence than intended by this objective. This phrase is not mentioned in paragraph 59; "verification of relevant security concepts_in future contracts for industrial control system hardware,".

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT has incorporated 'Risk Management' wording throughout the SAR. The SDT has revised the description for Objective 3 to address this comment. The phrase *at a minimum* in the description of objective 4 is from Order No. 829 (P 45). Because this is a SAR, the wording does not convey an obligation on entities. Oncor's comment will be considered during standards development.

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes

Comment

Occidental Chemical Corporation agrees with the proposed scope of Project 2016-03 as described in the SAR but offers the following suggestions:

- Purpose section of SAR states that the project will cover "security controls for supply chain management" but should probably be revised to state that it will cover "security controls for supply chain *risk* management" to be consistent with FERC Order 829 and the Industry Need section of the SAR.

• Purpose section of SAR states that the new or modified Reliability Standard(s) will require entities to "develop and implement a plan" – the SAR shouldn't assume that the agreed upon approach will be a "plan" and should be revised to read "develop and implement measures". This will allow the SDT the most flexibility if it is later determined that a "plan" is not the best approach and will still allow for a "plan" if the entity determines that to be the best approach	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has incorporated 'Risk Management' wording throughout the SAR. The purpose states that entities will be required to *develop and implement a plan*, which aligns with Order No. 829 directives (P 43 and 45). The SAR provides for the development of an equally effective and efficient alternative, which could include requirements for implementing measures instead of a plan.	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	Yes
Comment	
Thank you for this opportunity to provide comments on the Standards Authorization Request (SAR) written in response to Order No. 829 that will direct the development of a new or modified Reliability Standard for supply chain risk management to industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations. While FERC clearly wants to advance the state of supply chain security, we believe the inclusion of Low Impact Cyber Assets will delay the SDT's ability to make the one year filing deadline. We believe the SAR should narrow its focus to the 'highest watermark' first, to limit confusion, especially as entities prepare for implementing activities that address the Low Impact aspects of their programs. Other SDTs continue to enhance related NERC CIP standards based on changes to the definitions for Low Impact External Routable Connectivity and Transient Cyber Assets. All security advances and efficiencies designed for large-sized utilities, including their choice of software and hardware vendors, will eventually pass down to the Medium Impact Facilities, and ultimately to the Low Impact Facilities, through better IT security testing and best practices. This natural progression takes time and maturity to nurture, something we feel should be allowed reflected within in the SAR.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT will consider ACES' comments concerning Low Impact Cyber Assets during standards development.	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance	
Answer	Yes
Comment	
Objective 3 – Regarding Information System Planning - What is Information System Planning? It is not well understood. The SAR information does not adequately describe that beyond entities needing to document the risks we take into consideration. We would like to see additional description on Information System Planning.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will consider LCRA's comment during standards development.	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Comment	
PJM agrees with the language within the Project 2016-03 Cyber Security Supply Chain Management SAR and asks the SDT to consider the following comments when developing the standard. As stated within paragraph 42 of the order, PJM agrees with the APPA that the standard should be risk based as opposed to impact based. PJM also asks the SDT to consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within addressing the four objectives outlined in the order or by adding an additional objective.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments. The SDT will consider PJM's comments during standards development.	
Sophia Combs - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Comment	

Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Comment	

Likes 0	
Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Coon - Open Access Technology International, Inc. - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	Yes

Comment	
Likes 0	
Dislikes 0	
Response	

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance	
Answer	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Comment	
The IRC members ask the Standard Drafting Team (SDT) to consider the following comments when developing the standard. As stated within paragraph 42 of the order, the IRC members agree with the APPA that the standard should be risk based as opposed to impact based. The IRC members also ask the SDT to consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within the four objectives outlined in the order or by adding an additional objective.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider IRC's comments during standards development.	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	

Answer	
Comment	
Reclamation recommends that the CIP language be written to account for existing Government procurement constraints; or exempt the government entities that are legally bound by federal procurement regulations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider U.S. Bureau of Reclamation's comments during standards development.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Michelle Coon - Open Access Technology International, Inc. - NA - Not Applicable - NA - Not Applicable	
Answer	
Comment	
Open Access Technology international, Inc. (OATI) appreciates this opportunity to submit comments pertaining to the Cyber Security Supply Chain Management Standards Authorization Request (SAR). Tackling such a large and important issue is no easy feat. Yet, the standard drafting	

team has already demonstrated their commitment to this difficult and important task by creating a new draft standard for the most recent technical conference. Continued dedication to this effort will help ensure the new reliability standard is consistent and equally applicable to necessary areas of the bulk electric system.

As a committed provider of software solutions and services to the electric utility sector, OATI plans to participate in the standard drafting process to the fullest extent possible. There are significant challenges ahead that can benefit from OATI's perspective into all of the various aspects of the electric utility reliability. OATI has identified two significant challenges: consistency in application and manageability.

OATI observes a need to develop a consistent approach to applying this standard across the industry, large and small vendors, niche and cross-sector vendors. This will include taking into consideration the fact that some vendors which also focus heavily in other industries, may be less willing to accommodate a utility's need to meet this new NERC reliability standard. Smaller utilities, especially, could be presented with a "take it or leave it" proposition from vendors such as Microsoft, CISCO, or Dell. Additionally, there is a special issue presented by the widespread use of open source software in many software solutions today. A standard should not apply only to one subset of vendors/software. Rather, to avoid a discriminatory impact, the standard should be equally applicable to all in-scope vendors/ software solutions. While this issue of consistency presents many challenges, OATI stands eager to share ideas for reaching a reasonable resolution.

Another related challenge is one of manageability. To facilitate a manageable approach, OATI observes a need for NERC to establish a common baseline standard applicable to all in scope vendors/software. This should help avoid issues on both sides of the supply chain. Absent a baseline, utilities may each develop a variety of inconsistent approaches to meeting the objectives of the standard. Such inconsistency is likely to create major problems for vendors as they verify compliance with the standard. The downstream impact of such inconsistent approaches is an increased burden on vendors who may each develop a unique way to meet the objectives passed onto them. Fortunately, much work has already been completed by the Department of Energy and the National Institute of Standards and Technology in this area of supply chain security that will be helpful in defining the baseline for this industry. These existing approaches should be considered and leveraged in the development of this new CIP supply chain management standard.

OATI looks forward to working closely with NERC, industry members, and other vendors in shaping this new reliability standard. A special thanks to NERC for its inclusion of the vendors in this important and necessary effort. Together we can successfully develop a consistent and manageable standard to mitigate this cybersecurity vulnerability in the bulk electric system.

Likes 0	
Dislikes 0	

Response. Thank you for your comments and involvement in the standards development process.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	
Comment	
We also recommend that the SDT seriously consider updating existing CIP Standards in order to avoid creating double jeopardy for A) remote access (CIP-005 R2); B) patch management (CIP-007 R2); C) authentication (CIP-007 R5); D) vendor termination of employees (CIP-004 R5); We recommend that new Requirements do not jeopardize existing Requirements and their implementation timelines, and that new Requirements do not create additional paperwork with little value to the Reliable Operation of the Bulk Electric System.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT is considering both development of new standards, and revisions to existing standards, in determining how to address the directives in Order No. 829. The SDT will consider NPCC's comments during standards development.	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	
Comment	

If the SDT proposes to modify Low Impact requirements, we recommend maintaining them in Attachment 1 of NERC Standard CIP-003-6. Additions to Section 3: Access Controls could be made for future patch management requirements. We believe Section 4: Cyber Security Incident Response could be modified to include vendor remote termination access within a specified timeframe. The new definition of Transient Cyber Device could also be used as the location for baseline configuration management.

We believe all Low Impact processes should be non-prescriptive and provide flexibility for registered entities to decide how to best defend against cyber security threats based on their risk analysis. There may be significant advantages and protection for industry to adopt new supply chain requirements for those entities that have multiple vendors and large support staff. We believe that BES risks and economies of scale for G&T cooperatives are minimal, based on their size and geographical location within the BES.

Thank you for your time and attention regarding this SAR.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT will consider ACES comments during standards development.

Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF

Answer	

Comment

ITC Holdings finds this new standard to be ovrely burdensome for smaller utilities that do not have the infrastructure or staffing to perform the activities.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT is developing requirements to address directives in Order No. 829. Your comments will be considered during standards development.

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Comment	
The IESO suggests the Standard Drafting Team (SDT) consider the following comments when developing the standard. As stated within paragraph 42 of the order, the IESO agrees that the standard should be risk based as opposed to impact based. The IESO also suggests the SDT consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within the four objectives outlined in the order or by adding an additional objective.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider IESO's comments during standards development.	
Thomas Foltz - AEP - 3,5	
Answer	
Comment	
AEP suggests that any supply chain cyber security requirements applicable to low impact BES Cyber Systems be written in a revised CIP-003, Requirement R2, Attachment 1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider AEP's comments during standards development.	
Michael Shaw - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance	

Answer	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Comment	
We would like to point out the potential need for future modifications on other CIP standards as a result of this project. Specifically, there may be some language conflicts that arise, or duplicative controls put in place. Also, some ability will need to be afforded to entities allowing for the capability of verifying with a vendor, the integrity and authenticity of its software. Next, we feel like the language in the SAR should be revised to reflect a concentration on security controls for supply chain risk management, rather than just security controls for supply chain management. We feel the added emphasis on risk is appropriate in this context. Lastly, we want to point out to the drafting team the importance of keeping separate the topics of operations versus supply chain. We can see where instances may occur wherein the language of a standard can be intended to focus on supply chain aspects, but to the reader, may bleed over into the operations space.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider Duke's comments during standards development.	

The SDT has incorporated 'Risk Management' wording throughout the SAR.
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer
Comment
This SAR, if approved, allows the Standards Drafting Team (SDT) to develop new or modified Critical Infrastructure Protection (CIP) Standard(s) for supply chain management to address the Federal Energy Regulatory Commission (FERC) directives contained in Order No. 829. Texas RE supports developing new CIP Standard(s) to address supply chain management, which should be applicable to high, medium, and low impact BES Cyber Systems. Modifying existing CIP Standard(s) has caused confusion in the industry in regard to implementation dates. For example, CIP-003-6, added low impact Requirements, with multiple implementation dates.
Likes 0
Dislikes 0
Response. Thank you for your comments. The SDT will consider Texas RE's comments during standards development.

Standard Development Timeline

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

Description of Current Draft

This is the first draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016

Anticipated Actions	Date
45-day formal comment period with ballot	January 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

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

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

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

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

5. Effective Date: See Implementation Plan.

B. Requirements and Measures

Rationale for Requirement R1:
The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes controls for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to BES Cyber Systems and, to the extent applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan.

Requirement R1 Part 1.1 addresses Order No. 829 directives for identification and documentation of risks in the planning and development processes related to proposed BES Cyber Systems (P. 56). The objective is to ensure entities consider risks and options for mitigating these risks when planning, acquiring, and deploying BES Cyber Systems.

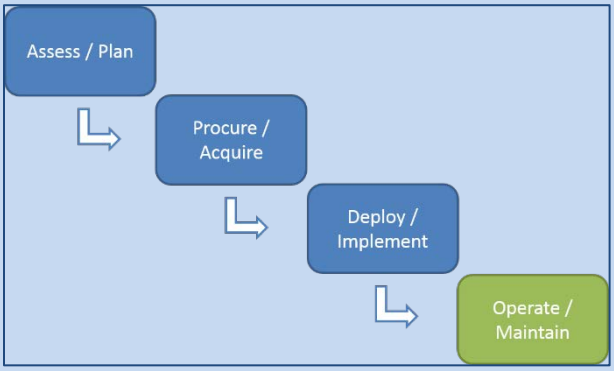
Requirement R1 Part 1.2 addresses Order No. 829 directives for procurement controls to address vendor-related security concepts in future contracts for BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 is accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to ensure that the software being installed in the applicable cyber system was not modified without the awareness of the software supplier and is not counterfeit.

The term *vendors* as used in the standard includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of Requirement R1 and R2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle.

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. The use of controls in BES Cyber System planning and development to:

1.1.1. Identify and assess risk(s) during the procurement and deployment of vendor products and services; and

1.1.2. Evaluate methods to address identified risk(s).

1.2. The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:

1.2.1. Process(es) for notification of vendor security events;

1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3. Process(es) for disclosure of known vulnerabilities;

1.2.4. Coordination of response to vendor-related cyber security incidents;

1.2.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

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

1.2.7. Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

M1. Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for mitigating cyber security risks as specified in the Requirement; and (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk management plan(s).

Rationale for Requirement R2:
The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Order No. 829 also directs that the periodic assessment "ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities" (P. 47). Examples of sources of information that the entity considers include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

R2. Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

2.1. Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and

2.2. Obtaining CIP Senior Manager or delegate approval.

M2. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s) and evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures as specified in the Requirement. Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

Rationale for Requirement R3:
The proposed requirement addresses Order No. 829 directives for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The 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.

R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

3.1. Operating System(s);

3.2. Firmware;

3.3. Commercially available or open-source application software; and

3.4. Patches, updates, and upgrades to 3.1 through 3.3.

M3. Evidence shall include (i) a documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation that the entity performed the actions contained in the process to verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to installation on high and medium impact BES Cyber Systems.

Rationale for Requirement R4:
The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective of the Requirement is to mitigate potential risks of a compromise at a vendor from traversing over an unmonitored remote access connection.

The objective of Requirement R4 Part 4.3 is for entities to have the ability to rapidly disable remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **4.1.** Authorization of remote access by the Responsible Entity;
- **4.2.** Logging and monitoring of remote access sessions to detect unauthorized activity; and
- **4.3.** Disabling or otherwise responding to unauthorized activity during remote access sessions.

M4. Evidence shall include (i) a documented process(es) for controlling vendor remote access as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation of authorization of vendor remote access; hard copy or electronic logs of vendor-initiated Interactive Remote Access and system-to-system remote access sessions; hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.

Rationale for Requirement R5:
The proposed requirement addresses Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems. (P. 48 and P. 51).

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

An entity could apply process(es) used for Requirements R3 and R4 to satisfy its obligations in Requirement R5 or could develop a separate policy or process(es) to address low impact BES Cyber Systems.

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

5.1. Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and

5.2. Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).

M5. Evidence may include, but is not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate for each cyber security policy.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:
"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:
The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

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

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

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	N/A	N/A	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include one of the elements specified in Parts 1.1 or 1.2.	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include either of the elements specified in Parts 1.1 or 1.2.; OR The Responsible Entity did not implement one or more documented supply chain risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 17 calendar months but less than or equal to 18	The Responsible Entity did not review and update, as necessary, its supply chain cyber security risk management plan(s) and obtain CIP Senior Manager or delegate approval within 18 calendar months of the previous review as specified in the Requirement.

	since the previous review as specified in the Requirement.	since the previous review as specified in the Requirement.	calendar months since the previous review as specified in the Requirement.	
R3.	N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.
R4.	N/A	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include one of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include two of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include any of the elements specified in Part 4.1 through Part 4.3; OR, The Responsible Entity did not implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems as

				specified in the Requirement.
R5.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 16 calendar months but less than or equal to 17 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include one of the elements in Parts 5.1 or 5.2; OR The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 17 calendar months but less than or equal to 18 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include either of the elements in Parts 5.1 or 5.2; OR The Responsible Entity did not have cyber security policies that were reviewed and approved by the CIP Senior Manager or delegate as specified in the requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 829	NA

Standard Attachments

None

Guidelines and Technical Basis

Rationale

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard CIP-013-1

Applicable Standard(s)

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

None

Prerequisite Standard(s)

None

Applicable Entities

CIP-013-1 — Cyber Security — Supply Chain Risk Management

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
  - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing 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 Bulk Electric System (BES) operations. Order No. 829 (at P 2) states:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

FERC directed NERC to submit the new or modified Reliability Standard within one year of the effective date of Order No. 829, i.e., by September 27, 2017.

General Considerations

Consistent with the directive to develop a forward-looking Reliability Standard, the implementation of CIP-013-1 does not require the abrogation or re-negotiation of contracts with vendors, suppliers or other entities executed as of the effective date of CIP-013-1 (See FERC Order No. 829, P. 36).

Effective Date

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Where approval by an applicable governmental authority is required, the standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the effective date of the applicable governmental authority's order approving the standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the standard shall become effective on the first day of the first calendar quarter that is twelve (12) months after the date the standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

Requirement R2

The initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 must be completed within fifteen (15) calendar months of the effective date of CIP-013-1.

Definition

None

Retirement Date

None

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Risk Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on proposed **CIP-013-1 – Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing 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 Bulk Electric System (BES) operations as follows:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

Questions

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

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you

agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or

if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

☐ Yes
☐ No
Comments:

9. Provide any additional comments for the SDT to consider, if desired.
Comments:

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-03 — Cyber Security — Supply Chain Risk Management

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **Project 2016-03 — Cyber Security — Supply Chain Risk Management.** Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines. The Emergency Operations Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report
FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in an Operations Planning time frame to develop one or more documented supply chain cyber security risk management plan(s). If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective, which is to develop one or more documented supply chain cyber security risk management plan(s). Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-013-1, R1			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include one of the elements specified in Parts 1.1 or 1.2.	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include either of the elements specified in Parts 1.1 or 1.2.; OR The Responsible Entity did not implement one or more documented supply chain risk management plan(s) as specified in the Requirement.

VRF Justifications for CIP-013-1, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VRF Justifications for CIP-013-1, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to develop one or more documented supply chain cyber security risk management plan(s) that set forth the controls.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in Operations Planning time frame that requires entities to implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. If violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and	The Responsible Entity did not review and update, as necessary, its supply chain cyber security risk management

obtained CIP Senior Manager or delegate approval but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	obtained CIP Senior Manager or delegate approval but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	obtained CIP Senior Manager or delegate approval but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	plan(s) and obtain CIP Senior Manager or delegate approval within 18 calendar months of the previous review as specified in the Requirement.

VSL Justifications for CIP-013-1, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R2 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R2	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	R3 is a requirement in Operations Planning time frame that requires the Responsible Entity to implement one or more documented process(es) for software integrity and authenticity controls to address risks from compromised software and firmware on high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R3 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R3			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R4 is Severe which is consistent with binary criteria. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	Only a Severe VSL is assigned.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-01, R4	
Proposed VRF	**Medium**
NERC VRF Discussion	R4 is a requirement in an Operations Planning time frame to implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R4 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R4			
Lower	**Moderate**	**High**	**Severe**
N/A	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include one of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include two of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include any of the elements specified in Part 4.1 through Part 4.3; OR The Responsible Entity did not implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems as specified in the Requirement.

VSL Justifications for CIP-013-1, R4	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R4 is not binary. Guideline 2b: The proposed VSLs do not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-013-1, R4	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R5	
Proposed VRF	**Lower**
NERC VRF Discussion	R5 is a requirement in Operations Planning time frame that requires the Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems to have one or more documented cyber security policies to address software integrity and authenticity and vendor remote access for its low impact BES Cyber Systems. If violated, it would not, under the emergency, abnormal, or restorative conditions anticipated by the policies, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Lower is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R5 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation

VSLs for CIP-013-1, R5			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 16 calendar months but less than or equal to 17 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include one of the elements in Parts 5.1 or 5.2; OR The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 17 calendar months but less than or equal to 18 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include either of the elements in Parts 5.1 or 5.2; OR The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review.

VSL Justifications for CIP-013-1, R5	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R5 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R5	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

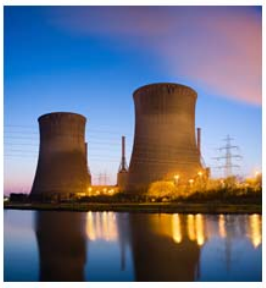
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Guidance and Examples

DRAFT CIP-013-1 – Cyber Security - Supply Chain Risk Management

January 17, 2017

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Introduction

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (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 Bulk Electric System (BES) operations as follows:

> *[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.*

The Commission established a filing deadline of one year from the effective date of Order No. 829, which is September 27, 2017.

The Commission also explains that it "does not require NERC to impose any specific controls nor does the Commission require NERC to propose 'one-size-fits-all' requirements." (P 13)

> *Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., 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"))*

Furthermore, FERC clarified the scope of the directives in Order No. 829 by stating (P 21):

> *we reiterate the statement in the NOPR that 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."*

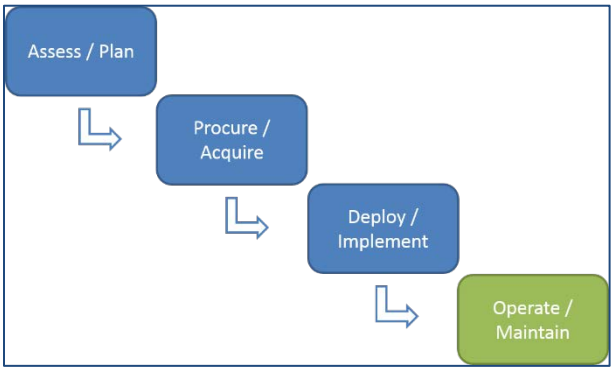
This technical reference provides a summary of the CIP-013-1 framework, which includes a description of the requirements that meet FERC's directives, including each of the objectives; the risk each objective is intended to address; some considerations for implementing the requirements; and examples of controls that responsible entities could use to meet the requirements.

CIP-013-1 Framework

Consistent with the Commission's directives, CIP-013-1 requires that responsible entities address each of the objectives set forth in Order No. 829 by developing and implementing a cyber security risk management plan and documented operating processes to protect against supply chain risks. The proposed standard is forward looking in that it does not require entities to renegotiate currently effective contracts in order to implement their plan.

Collectively, the provisions of Requirement R1 and R2 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle. The term *vendors* as used in the standard includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Responsible Entities

Proposed CIP-013-1 uses the same applicability as found in other CIP cyber security standards.

Requirement R1

R1. *Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address:*

1.1. *The use of controls in BES Cyber System planning and development to:*

1.1.1. *Identify and assess risk(s) during the procurement and deployment of vendor products and services; and*

1.1.2. *Evaluate methods to address identified risk(s).*

1.2. *The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:*

1.2.1. *Process(es) for notification of vendor security events;*

1.2.2. *Process(es) for notification when vendor employee remote or onsite access should no longer be granted;*

1.2.3. *Process(es) for disclosure of known vulnerabilities;*

1.2.4. *Coordination of response to vendor-related cyber security incidents;*

1.2.5. *Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;*

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

1.2.7. *Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.*

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes controls for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (P 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to BES Cyber Systems and, to the extent applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. These cyber systems cover the scope of assets needed to address FERC Order No. 829 directives, which specified that the standards must address supply chain risks to "industrial control system hardware, software, and computing and networking services associated with bulk electric system operations" (P 43).

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.

To achieve the flexibility needed for supply chain cyber security risk management, responsible entities could use a "risk-based approach" to addressing the objectives. One example of a risk-based cyber security risk management plan is system-based, which describes specific controls for high, medium, and low impact BES Cyber Systems. Another example of a risk-based approach is vendor-based, allowing entities to develop its plan(s) around risk posed by various vendors of its BES Cyber Systems. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (P 44)."

Objective: Information System Planning and Procurement

Requirement R1 Part 1.1 addresses Order No. 829 directives for identification and documentation of risks in the planning and development processes related to proposed BES Cyber Systems (P 56). The objective is to ensure entities consider risks and options for mitigating these risks when planning, acquiring, and deploying BES Cyber Systems.

Requirement R1 Part 1.2 addresses Order No. 829 directives for procurement controls to address vendor-related security concepts in future contracts for BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets (P 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 is accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.

Security Risks in Information System Planning and Procurement

The objective addresses risks identified in Order No. 829 (P 57):

> *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.*

FERC also cited to the BlackEnergy malware campaign that used a zero day vulnerability (previously unknown) to remotely execute malicious code on devices that contain this vulnerability. Steps to "(1) minimize network exposure for all control system devices/subsystems; (2) ensure that devices were not accessible from the internet; (3) place devices behind firewalls; and (4) utilize secure remote access techniques" during system development and planning could mitigate such risk (P 57).

The objective also addresses additional risks identified in Order No. 829 (P 60):

> *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. In addition, this objective addresses the risk that a compromised vendor would not provide adequate notice and related incident response to responsible entities with whom the vendor is connected.*

Entity Considerations in Meeting the Objective

In implementing Requirement R1, the responsible entity should consider the following:

- Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
- Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes reviewed and evaluated during the planning, bidding, evaluation and contracting phases of the procurement process.
- Using periodic review processes with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
- Vendor or service provider use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service provider security practices.
- Using third parties to conduct security assessments and penetration testing for specific vendors or "cloud based" service providers.
- Vendor supply chain channels and plans to mitigate potential risks or disruptions.
- Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
- Corporate governance and approval processes. Consider establishing additional controls based on risk.
- Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
- Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
- Use of procurement controls to aid with vendor risk assessments and mitigation measures for cyber security during the procurement process.

In implementing procurement controls, especially contract terms, responsible entities should be careful not to limit their negotiating ability with vendors through their CIP-013-1 plans. An example of this would be a procurement control that requires specific contract terms. This may have unintended consequences such as significant and unexpected cost increases for the product or service or vendors walking away from contracts.

Responsible entities may use their entire procurement process (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) rather than just contract terms to help them meet the objective and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks.

Obtaining the desired specific cyber security controls in the negotiated contract may not be feasible with each vendor. Baseline controls should be established with the knowledge that every negotiated contract will be different. Factors such as competition, sole source of supply, or supplier's progression will determine the negotiated outcomes of the contract. This variation in contract terms is anticipated and is not considered failure to implement an entity's plan. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the entity may explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems.

Potential Information System Planning Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are some examples of controls:

1.1. *The use of controls in BES Cyber System planning and development to:*

1.1.1. *Identify and assess risk(s) during the procurement and deployment of vendor products and services; and*

- Responsible Entity can develop plans to identify potential cyber security risks during the information system planning, system development, acquisition and deployment lifecycle processes. The plans can define the required security controls within the lifecycle that address threats, vulnerabilities, adverse impacts and risk to BES Cyber Systems.
- Participation of identified cross-organizational subject matter experts with appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal to be included in the planning and acquisition process.
- Identify potential risks based on information systems, system components, and/or information system services / integrators.
- Assess vendors based on their risk management controls. Examples of vendor risk management controls to consider include[1]:
  - Personnel background and screening practices by vendors
  - Training programs and assessments of personnel on cyber security
  - Formal security programs which include their technical, organizational, and security management practices
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle
  - Review of vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles)
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout their processes
  - Review of certifications and their alignment with recognized industry and regulatory controls
  - Summary of any internal and independent cyber security testing performed on the products to ensure secure and reliable operations. Ask vendors to share third-party/independent product testing results during the request for proposal stage of acquisition process
  - Understand product roadmap to determine vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support
  - Define any critical elements or components that may impact the operations or reliability of BES Cyber Systems

[1] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

- Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. This may include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Identify any components of products that are not owned and managed by the vendor that may introduce additional risks, such as use of open source code or third party developers and manufacturers.

- Plan for information systems component end-of-life or discontinuation of product support. Define plans for replacement when support from the developer, vendor, or manufacturer is no longer provided. Provide justification and documented approval for the continued use of system components required to satisfy mission needs and ensure ongoing cyber security protection and reliability. (see NIST SP 800-53 SA-22 – Unsupported System Components)

1.1.2. *Evaluate methods to address identified risk(s).*

- Based on risk assessment, determine mitigating controls that can be applied in procurement and/or operation phase of product or service acquisition and implementation. Examples include:
  - Hardening the information systems and minimizing the attack surface vulnerabilities introduced with vendor products and services.
  - Ensure ongoing support and availability of system components for duration of expected life of products. Define the primary and alternate sources (if any) of components, parts and support services.
  - Controls to ensure system components, parts and support services are only acquired through trusted sources.
  - Identify alternative vendors that may supply critical elements and components, provide support services, or offer equivalent business functional solutions.
  - Review and address other risks in Requirement R1 Part 1.1.1.

Potential Procurement Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are examples of some controls:

1.2. *The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:*

- Responsible Entity can define cyber security terms in the procurement request for proposal (RFP) for BES Cyber Systems to ensure the vendor(s) understands the cyber security expectations and implements proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle. An example set of baseline supply chain cyber security procurement language for use by BES owners operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG). Each Responsible Entity will need to determine the applicability of these sample terms and how such terms may complement other cyber security expectations in a clear and measurable manner.

- During negotiations of procurement contracts, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security

procurement language that is applicable to the supplier's system component, system integrators, or external service providers.

1.2.1. *Process(es) for notification of vendor security events;*

- Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems.
- Security Event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Notifications could include information on (i) mitigating controls that may be implemented by Responsible Entity, (ii) availability of patch or corrective components.
- Security Event notifications to the vendor should be sent to designated point of contact as determined by the vendor. Vendor should respond within a defined timeframe with information on (i) mitigating controls that may be implemented by Responsible Entity, (ii) availability of patch or corrective components.

1.2.2. *Process(es) for notification when vendor employee remote or onsite access should no longer be granted;*

- Using contract language, the Responsible Entity can maintain the right in its sole discretion to suspend or terminate remote or onsite access of vendor, or any individual employee of vendor, at any time without further notice for any reason. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- Request vendor cooperation in obtaining Responsible Entity notification of when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination.
- If vendor utilizes third parties to perform services to Responsible Entity, request vendor cooperation to obtain Responsible Entity's prior approval and third party adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.3. *Process(es) for disclosure of known vulnerabilities;*

- Review vendor summary documentation of publicly disclosed vulnerabilities in the procured product and the status of the vendor's disposition of those publicly disclosed vulnerabilities.
- Request vendor cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- After contract award and for duration of relationship with vendor, request vendor cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain. Documentation should include a summary

description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.

1.2.4. *Coordination of response to vendor-related cyber security incidents;*

- Responsible Entity can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with Responsible Entity in implement mitigating controls and product corrections.
- In the event the Responsible Entity identifies a security incident that may or has resulted in an adverse impact to the availability or reliability of BES Cyber Systems, the Responsible Entity will seek vendor cooperation on notification processes, assistance and support requirements from the vendor.
- In the event the vendor identifies a vulnerability that has resulted in a cyber security incident related to the products or services provided to the Responsible Entity, vendor should provide notification to Responsible Entity per contract agreements. The vendor could provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks.
- Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.5. *Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;*

- Request access to vendor documentation detailing the vendor patch management program and update process for all system components (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity.
- Request access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- For duration of the product life cycle, require vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- Request vendors provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- Request vendors describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- When third-party components are provided by the vendor, request vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses.

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

- Request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- Request vendors maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- Request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- For vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, request vendors maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

1.2.7. *Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.*

- Request vendors provide Responsible Entity with audit rights that allow the Responsible Entity or designee to audit vendor's security controls, development and manufacturing controls, access to certifications and audit reports, and other relevant information.
- If vendor is not the original manufacturer of the products, require the vendor to certify that replacement parts supplied are made by the original equipment manufacturer and meet the applicable manufacturer data sheet or industry standard.
- For any replacement parts that vary from OEM specifications, request the vendor obtain prior approval by the Responsible Entity before substitution. Consider requiring vendor to provide testing certification or specifications that the replacement parts meet original product requirements.
- Require vendor to use designated or trusted providers for product delivery and services.
- Restrict the use and publication of Responsible Entity information in contracts, e.g., do not allow suppliers to publish your entity name, products or services on their websites or in sales materials.

Requirement R2

R2. *Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include:*

2.2. *Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and*

2.3. *Obtaining CIP Senior Manager or delegate approval.*

Objective: Review Supply Chain Cyber Security Risk Management Plans

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Order No. 829 also directs that the periodic assessment "ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities" (P. 47). Examples of sources of information that the entity considers include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Entity Considerations in Meeting the Objective

Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review. In the Requirement R2 review, responsible entities must consider new risks and available mitigation measures, which could come from a variety of sources that may include NERC, DHS, and other sources. The requirement also requires the identification of changes made, if any, to the controls based on this review.

CIP-003-6, Requirements R3 and R4 address the identification and delegation process for the CIP Senior Manager for this and the other CIP Standards.

Potential Supply Chain Cyber Security Risk Management Plan Controls

Responsible Entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

2.1. *Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and*

- Responsible Entity will maintain a documented supply chain cyber security risk management plan
- Cross-organizational representative subject matter experts from appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. should collaboratively develop and be responsible to review the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Considerations for changes may include:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), NIST).

- Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
- Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned. Examples may include changes to contract terms based on market maturity, capabilities, and cyber security advancements.

- Development of communications or training material to ensure any organizational areas affected by revisions to the supply chain cyber security risk management plan(s) are informed.

2.2. *Obtaining CIP Senior Manager or delegate approval.*

- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Entities may incorporate the review into their annual CIP-003 review.
- Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals.

Requirement R3

R3. *Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems:*

- **3.1.** *Operating System(s);*
- **3.2.** *Firmware;*
- **3.3.** *Commercially available or open-source application software; and*
- **3.4.** *Patches, updates, and upgrades to 3.1 through 3.3.*

Objective: Software Integrity and Authenticity

The proposed requirement addresses Order No. 829 directives for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48). The 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.

Security Risks from Compromised Software

The Objective addresses the risk that an attacker could exploit legitimate vendor software delivery or patch management processes to deliver compromised software updates or patches to a BES Cyber System. [2] In Order No. 829, FERC provides additional context to this risk by stating that adequate authenticity and integrity controls could prevent malware campaigns or "Watering Hole" attacks that target the exploitation of vulnerable patch management processes.[3]

Entity Considerations in Meeting the Objective

In implementing Requirement R3, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used by their vendors to deliver software and appropriate control(s) that will verify the integrity and authenticity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software integrity and authenticity can be verified through those processes.
- Integration of procurement controls from the responsible entity's supply chain cyber security risk management plan as identified in Requirement R1. During procurement of new systems, such as systems with preinstalled software, ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt.
- Coordination of the responsible entity's integrity and authenticity control(s) with other cyber security policies and controls, including change management and patching processes, procurement controls, and incident response plans.
- Use of a secure central software repository after software authenticity and integrity have been validated, so that authenticity and integrity checks do not need to be performed before each installation.

[2] *Id.* at P 48 and P 49. "This 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" *(P 49).* FERC explains that the objective applies to all software (P 48).

[3] *Id.*

- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the responsible entity.

Potential Software Integrity Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

- Prior to installing software or placing software into operation on a BES Cyber System, verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require vendors to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the vendor.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Potential Software Authenticity Controls

Responsible entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

- Obtain software from an authenticated source before installation.
- Prior to installing software or placing software into operation on a BES Cyber System, verify that the software has been digitally signed and validate the signature to ensure that the software is authentic.
- Use public key infrastructure (PKI) with encryption to ensure that the software is authentic by enabling only intended recipients to decrypt the software.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping).

Requirement R4

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1. Authorization of remote access by the Responsible Entity;

4.2. Logging and monitoring of remote access sessions to detect unauthorized activity; and

4.3. Disabling or otherwise responding to unauthorized activity during remote access sessions.

Objective: Vendor Remote Access to BES Cyber Systems

The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective of the Requirement is to mitigate potential risks of a compromise at a vendor from traversing over an unmonitored remote access connection.

The objective of Requirement R4 Part 4.3 is for entities to have the ability to rapidly disable remote access sessions in the event of a system breach as specified in Order No. 829 (P 52).

Security Risk Related to Vendor Remote Access

The objective addresses risks identified in Order No. 829:

> *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.*[4]

Entity Considerations in Meeting the Objective

Requirement R4 Part 4.1 requires responsible entities to implement a control(s) to restrict vendor access, which includes access by a person or a machine. The control(s) used by a responsible entity may vary depending on entity-specific factors and existing cyber security policies (i.e. different entities grant varying levels and amounts of vendor remote access depending on entity needs.)

In addition to authorizing remote access, Requirement R4 requires the implementation of a control(s) to monitor vendor access (Part 4.2). Therefore, if a vendor is allowed to access BES Cyber Systems, then the responsible entity is required to monitor this access. This control(s) will address the Commission's concern that the responsible entity may not have the level of visibility over the remote access system-to-system session on the BES Cyber Systems, which could allow malicious intrusion attempts to take place.

Requirement R4 Part 4.3 addresses the detection of unauthorized (i.e., inappropriate) activity as well as the response to the detection of such activity, while allowing the responsible entity flexibility in the control(s) it uses to meet this part of the security objective.

It is important to recognize that these new requirements may be partially addressed by the responsible entity's existing remote access controls used to comply with approved CIP Standards. In implementing Requirement R4, the responsible entity should consider their existing CIP cyber security policies and controls.

[4] 156 FERC ¶ 61,050 at P 52.

For Requirement R4 Part 4.1, an entity may already have some authorization controls in place that will support meeting this objective.[5] If these controls do not fully cover vendor-initiated Interactive Remote Access and system-to-system remote access with a vendor(s), additional remote access controls are needed to meet the objective. For example, if an entity allows vendor remote access only during specific circumstances, such as response to system problems, the entity put other controls in place to disable vendor remote access at other times. Other entities may find that vendor remote access is required at all times and may use other controls as discussed below to achieve the objective. For example, the entity could employ operator-based controls that use various identification methods to control vendor remote access pathways into BES Cyber Systems.

For Requirement R4 Part 4.2, an entity may have monitoring controls in place for some BES Cyber Systems, however the controls may not necessarily address remote access session monitoring and alerting.[6] These existing monitoring controls could be enhanced to meet the objective. Entities should consider:

- Available capabilities and technologies for monitoring session activity with a vendor
- Setting up processes and parameters to monitor and log remote access login attempts to detect unauthorized remote access
- Development of procurement technical specifications for vendor remote access to support monitoring vendor remote access traffic during remote sessions

Entities may find it appropriate to modify their existing controls associated alert and response processes for Requirement R4 Part 4.3 including the threshold for alerting, persons alerted, as well as the timelines for alerting and responding. Entities may also find it appropriate to modify their existing controls and processes associated with CIP-008-5 - Cyber Incident Response Plan. Other considerations:

- Entity determination of appropriate response to unauthorized access from personnel, technology, and risk standpoints
- Thresholds for alerting, persons alerted, and the timelines for alerting and responding to unauthorized activity in order ensure reliable BES operations
- Availability and reliability of methods to prevent vendor remote access or disable vendor remote access sessions if unauthorized or illegitimate access is detected.

Potential Remote Access Controls

Responsible Entities may use various control(s) to address the security risk for this objective. Below are examples of potential controls:

<u>For Requirement R4 Part 4.1 (Authorization Controls):</u>

- Use an operator controlled, time limited (e.g., lock out, tag out) process for vendor remote access. Example approaches may include:
  - For user initiated sessions, use token authentication by authorized personnel. Token activation is for a specific timeframe or specific location. For machine-to-machine sessions, use encryption and multi-factor authentication that changes on a determined timeframe.

[5] For example, CIP-004-6 - Personnel and Training, which covers training and personnel risk assessment requirements, and CIP-007-6 Requirement 5 – System Access Control, which covers account access controls.

[6] CIP-005-5 Requirement R1.5 covers detection of malicious communications for medium and high BES Cyber Systems in Control Centers, and CIP-007-6 Requirements 4.1 and 4.2 covers logging of access and detection of failed access attempts.

- Designate specific timeframe access for the exchange of information. The responsible entity is responsible for ensuring access is terminated at the conclusion of the timeframe.
- Terminate access upon notification the underlying purpose has ended.
- Consider requiring vendors to specifically request remote access in order to support operator controlled and time limited access.

For Requirement R4 Part 4.2 (Logging and Monitoring Controls):

- Set up logging and monitoring parameters on key attributes and thresholds as appropriate, such as number of failed log-in attempts.
- Log and monitor vendor remote access sessions and review logs for abnormal behavior. Have a method for terminating suspicious sessions.
- Consider extended use of jump hosts for access to protected networks (e.g. specific jump hosts dedicated to vendor remote access).
- Use monitoring and control mechanisms and processes at the boundary between the responsible entity and vendors (e.g. application level firewalls or intrusion detection/prevention systems).
- Change default parameters for authentication mechanisms (e.g., passwords) or access/network protocols prior to installing Cyber Assets.

For Requirement R4 Part 4.3 (Disable Access and Entity Response Controls):

- Set up alerting parameters and thresholds on key attributes as appropriate for the entity (e.g., number of failed login attempts or detection of inappropriate activities).
- Set up alerting and response processes so that inappropriate vendor remote access sessions may be disabled or otherwise responded to in a timely manner.

Requirement R5

R5. *Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:*

5.1. *Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and*

5.2. *Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).*

Objective: Software and Vendor Remote Access Risk Mitigation in Low Impact BES Cyber Systems

The proposed requirement addresses Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems. (P. 48 and P. 51).

Security Risks

Preceding sections discuss the related risks as identified in Order No. 829. Requirement R5 is intended to address these risks as they apply to low impact BES Cyber Systems. Responsible Entities have flexibility to use an approach for low impact BES Cyber Systems that is different from the approach used for medium and high impact BES Cyber Systems.

Entity Considerations for Meeting the Objective

In implementing Requirement R5, the responsible entity should consider the following:

- Considerations and controls for addressing software risks and vendor remote access risks to high and medium impact BES Cyber Systems discussed above that the entity determines are also applicable to its low impact BES Cyber Systems.
- Entity processes for addressing software risks and vendor remote access risks per Requirements R3 and R4. Consider whether to include low impact BES Cyber Systems in these processes, or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber Systems.
- Existing CIP cyber security policies and controls that can be included or referenced in a cyber security policy to meet the objective. For example, some electronic access controls established by an entity for low impact BES Cyber Systems pursuant to approved CIP-003 requirements may be part of the cyber security policy specified in Requirement R5 for controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).
- Asset management factors applicable to the entity. Entities can develop its cyber security policies either by individual asset or by groups of assets. As noted in the rationale section of proposed CIP-013-1, an inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required.

Potential Controls for Cyber Security Policies to Meet the Objective

Responsible entities may use various control(s) to address the security risks for this objective. Below are examples of potential controls that an entity could include in its cyber security policy or process(es):

- Policies, procedures, and/or checklists for personnel to check that software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Policies, procedures, and/or checklists that support obtaining software from trustworthy sources.
- Policies for using trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)
- Policies, procedures, and/or checklists for applying other controls discussed above that address software risks and vendor remote access.

References

- Utilities Technology Council (UTC) “Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation”
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - “Cybersecurity Procurement Language for Energy Delivery Systems”

Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified 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.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.*
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed standard must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., 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")).	The directive is addressed by Requirements R1, R3, R4, and R5 of proposed CIP-013-1. Requirement R1 specifies that entities must implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle as described further below.

Order No. 829 Citation	Directive / Guidance	Resolution
		Proposed CIP-013-1 Requirement R1 **R1.** Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: **1.1.** The use of controls in BES Cyber System planning and development to: **1.1.1.** Identify and assess risk(s) during the procurement and deployment of vendor products and services; and **1.1.2.** Evaluate methods to address identified risk(s). **1.2.** The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets: **1.2.1.** Process(es) for notification of vendor security events;

Order No. 829 Citation	Directive / Guidance	Resolution
		1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted; **1.2.3.** Process(es) for disclosure of known vulnerabilities; **1.2.4.** Coordination of response to vendor-related cyber security incidents; **1.2.5.** Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use; **1.2.6.** Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and **1.2.7.** Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require 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. This periodic assessment should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	The directive is addressed in proposed CIP-013-1 Requirement R2. **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include: **2.1.** Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and

Order No. 829 Citation	Directive / Guidance	Resolution
		2.2. Obtaining CIP Senior Manager or delegate approval.
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	The directive is addressed in proposed CIP-013-1 Requirement R2 part 2.1 (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement R2:** Order No. 829 also directs that the periodic assessment "ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities" (P. 47). Examples of sources of information that the entity considers include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC) *Technical Guidance and Examples* document developed by the drafting team includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and Requirements R3 and R5 Part 5.1. Requirement R3 applies to high and medium impact BES Cyber Systems. Requirement R5 applies to low impact BES Cyber Systems. **Proposed CIP-013-1 Requirement R3** **R3.** Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and

Order No. 829 Citation	Directive / Guidance	Resolution
		firmware before being placed in operation on high and medium impact BES Cyber Systems: **3.1.** Operating System(s); **3.2.** Firmware; **3.3.** Commercially available or open-source application software; and **3.4.** Patches, updates, and upgrades to 3.1 through 3.3. **<u>Proposed CIP-013-1 Requirement R5</u>** **R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: **5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and...
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-013-1 Requirement R4 Part 4.1 and 4.2 and Requirement R5 Part 5.2. Requirement R4 applies to high and medium impact BES Cyber Systems. Requirement R5 applies to low impact BES Cyber Systems.

Order No. 829 Citation	Directive / Guidance	Resolution
		Proposed CIP-013-1 Requirement R4 **R4.** Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): **4.1.** Authorization of remote access by the Responsible Entity; **4.2.** Logging and monitoring of remote access sessions to detect unauthorized activity; and **4.3.** Disabling or otherwise responding to unauthorized activity during remote access sessions. **Proposed CIP-013-1 Requirement R5** **R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: **5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).

Order No. 829 Citation	Directive / Guidance	Resolution
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by Requirement R4 Part 4.3 (above) and Requirement R5 Part 5.2 (above).
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address 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. 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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).
Objective 4: Vendor Risk Management and Procurement Controls		
P 59	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. Specifically, NERC must address controls for the following topics: (1) vendor security event notification processes; (2) vendor personnel termination 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. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1

Formal Comment Period Open through March 6, 2017
Ballot Pools Forming through February 17, 2017

Now Available

A 45-day formal comment period for **CIP-013-1 - Cyber Security – Supply Chain Risk Management**, is open through **8 p.m. Eastern, Monday, March 6, 2017**.

Commenting

Use the electronic form to submit comments on the standard. If you experience any difficulties in using the electronic form, contact Nasheema Santos. An unofficial Word version of the comment form is posted on the project page.

Join the Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, February 17, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **February 24 – March 6, 2017**.

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

For more information or assistance, contact Senior Standards Developer, Mark Olson (via email) or at (404) 446-9760.

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

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/80)
Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 IN 1 ST
Voting Start Date: 2/24/2017 12:01:00 AM
Voting End Date: 3/6/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 325
Total Ballot Pool: 373
Quorum: 87.13
Weighted Segment Value: 10.36

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	96	1	8	0.101	71	0.899	0	3	14
Segment: 2	7	0.7	0	0	7	0.7	0	0	0
Segment: 3	82	1	6	0.085	65	0.915	0	2	9
Segment: 4	24	1	1	0.048	20	0.952	0	0	3
Segment: 5	87	1	8	0.113	63	0.887	0	1	15
Segment: 6	61	1	8	0.148	46	0.852	0	1	6
Segment: 7	3	0.3	0	0	3	0.3	0	0	0
Segment: 8	4	0.3	1	0.1	2	0.2	0	0	1
Segment: 9	1	0	0	0	0	0	0	1	0
Segment: 10	8	0.4	1	0.1	3	0.3	0	4	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	373	6.7	33	0.694	280	6.006	0	12	48

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Negative	Comments Submitted
1	Allete - Minnesota Power, Inc.	Jamie Monette		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Negative	Third-Party Comments
1	American Transmission Company, LLC	Lauren Price		Negative	Comments Submitted
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Negative	Comments Submitted
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Patricia Robertson		None	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Black Hills Corporation	Wes Wingen		Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Negative	Comments Submitted
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Negative	Comments Submitted
1	CPS Energy	Glenn Pressler		Negative	Comments Submitted
1	Dairyland Power Cooperative	Robert Roddy		Abstain	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Negative	Comments Submitted
1	El Paso Electric Company	Pablo Onate		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Chris Scanlon		Negative	Comments Submitted
1	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Negative	Comments Submitted
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Negative	Comments Submitted
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Negative	Third-Party Comments
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Negative	Comments Submitted
1	JEA	Ted Hobson	Joe McClung	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		Negative	Comments Submitted
1	Long Island Power Authority	Robert Ganley		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Los Angeles Department of Water and Power	faranak sarbaz		Negative	Comments Submitted
1	Lower Colorado River Authority	Teresa Cantwell		Negative	Comments Submitted
1	M and A Electric Power Cooperative	William Price		Negative	Third-Party Comments
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Negative	Third-Party Comments
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Negative	Third-Party Comments
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Third-Party Comments
1	National Grid USA	Michael Jones		Negative	Third-Party Comments
1	Nebraska Public Power District	Jamison Cawley		Negative	Third-Party Comments
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Third-Party Comments
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Third-Party Comments
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Third-Party Comments
1	Peak Reliability	Scott Downey		Affirmative	N/A
1	Platte River Power Authority	Matt Thompson		Negative	Comments Submitted
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Abstain	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Negative	Comments Submitted
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Third-Party Comments
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Negative	Third-Party Comments
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Third-Party Comments
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Negative	Comments Submitted
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Third-Party Comments
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Negative	Comments Submitted
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Negative	Third-Party Comments
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted
1	Tri-State G and T Association, Inc.	Tracy Sliman		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Negative	Third-Party Comments
1	Xcel Energy, Inc.	Dean Schiro		Negative	Third-Party Comments
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	ISO New England, Inc.	Michael Puscas		Negative	Third-Party Comments
2	Midcontinent ISO, Inc.	Terry BIlke		Negative	Comments Submitted
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Negative	Third-Party Comments
3	Ameren - Ameren Services	David Jendras		Negative	Third-Party Comments
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Negative	Comments Submitted
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	BC Hydro and Power Authority	Faramarz Amjadi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens	Darnez Gresham	Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Third-Party Comments
3	City of Farmington	Linda Jacobson-Quinn		Negative	Comments Submitted
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Negative	Third-Party Comments
3	Clark Public Utilities	Jack Stamper		None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Abstain	N/A
3	Colorado Springs Utilities	Hillary Dobson		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	El Paso Electric Company	Rhonda Bryant		None	N/A
3	Eversource Energy	Mark Kenny		Negative	Comments Submitted
3	Exelon	John Bee		Negative	Comments Submitted
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted
3	Great River Energy	Brian Glover		Negative	Third-Party Comments
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Abstain	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Negative	Comments Submitted
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Third-Party Comments
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Third-Party Comments
3	Modesto Irrigation District	Jack Savage	Nick Braden	Negative	Third-Party Comments
3	Muscatine Power and Water	Seth Shoemaker		Negative	Third-Party Comments
3	National Grid USA	Brian Shanahan		Negative	Third-Party Comments
3	Nebraska Public Power District	Tony Eddleman		Negative	Third-Party Comments
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Third-Party Comments
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Third-Party Comments
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Third-Party Comments
3	Ocala Utility Services	Randy Hahn		Negative	Third-Party Comments
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Third-Party Comments
3	Omaha Public Power District	Aaron Smith		Negative	Third-Party Comments
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Negative	Comments Submitted
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Negative	Third-Party Comments
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Mick Neshem		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Negative	Comments Submitted
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jeff Neas		None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Negative	Comments Submitted
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Third-Party Comments
3	Tennessee Valley Authority	Ian Grant		Negative	Comments Submitted
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Third-Party Comments
3	Westar Energy	Bo Jones		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Negative	Third-Party Comments
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Negative	Third-Party Comments
4	Austin Energy	Tina Garvey		Negative	Third-Party Comments
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Beth Fields		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Negative	Third-Party Comments
4	Illinois Municipal Electric Agency	Bob Thomas		Negative	Third-Party Comments
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Negative	Comments Submitted
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Negative	Comments Submitted
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	Third-Party Comments
4	Oklahoma Municipal Power Authority	Ashley Stringer		Negative	Third-Party Comments
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Third-Party Comments
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Third-Party Comments
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Negative	Third-Party Comments
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Third-Party Comments
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Third-Party Comments
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Colorado Springs Utilities	Jeff Icke		Negative	Comments Submitted
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Negative	Comments Submitted
5	CPS Energy	Robert Stevens		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Thomas Rafferty		Negative	Comments Submitted
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	El Paso Electric Company	Victor Garzon		Negative	Comments Submitted
5	Eversource Energy	Timothy Reyher		Negative	Comments Submitted
5	Exelon	Ruth Miller		Negative	Comments Submitted
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Negative	Comments Submitted
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		Negative	Third-Party Comments
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	JEA	John Babik		Negative	Third-Party Comments
5	Kissimmee Utility Authority	Mike Blough		Negative	Third-Party Comments
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	Comments Submitted
5	Los Angeles Department of Water and Power	Kenneth Silver		Negative	Comments Submitted
5	Lower Colorado River Authority	Wesley Maurer		Negative	Comments Submitted
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Negative	Comments Submitted
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Negative	Third-Party Comments
5	MEAG Power	Steven Grego	Scott Miller	Negative	Third-Party Comments
5	Muscatine Power and Water	Mike Avesing		Negative	Third-Party Comments
5	National Grid USA	Elizabeth Spivak		None	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Third-Party Comments
5	New York Power Authority	Erick Barrios		Negative	Comments Submitted
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Third-Party Comments
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Negative	Third-Party Comments
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Third-Party Comments
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Third-Party Comments
5	Omaha Public Power District	Mahmood Safi		Negative	Third-Party Comments
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Third-Party Comments
5	Platte River Power Authority	Tyson Archie		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Negative	Third-Party Comments
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Third-Party Comments
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		Negative	Third-Party Comments
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Negative	Comments Submitted
5	SunPower	Bradley Collard		Negative	Comments Submitted
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		None	N/A
5	Talen Generation, LLC	Donald Lock		Negative	Comments Submitted
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Third-Party Comments
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Negative	Third-Party Comments
5	Westar Energy	Laura Cox		None	N/A
5	Xcel Energy, Inc.	David Lemmons	Amy Casuscelli	Negative	Comments Submitted
6	AEP - AEP Marketing	Dan Ewing		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Paul Huettl		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Third-Party Comments
6	Black Hills Corporation	Eric Scherr		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	El Paso Electric Company	Luis Rodriguez		Negative	Comments Submitted
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Negative	Comments Submitted
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Negative	Comments Submitted
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Michael Brytowski	Negative	Third-Party Comments
6	Lakeland Electric	Paul Shipps		Negative	Third-Party Comments
6	Lincoln Electric System	Eric Ruskamp		Negative	Comments Submitted
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Negative	Comments Submitted
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Negative	Third-Party Comments
6	Muscatine Power and Water	Ryan Streck		Negative	Third-Party Comments
6	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Third-Party Comments
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Third-Party Comments
6	Omaha Public Power District	Joel Robles		Negative	Third-Party Comments
6	Platte River Power Authority	Sabrina Martz		Negative	Comments Submitted
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Negative	Third-Party Comments
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Third-Party Comments
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southeastern Power Administration	Douglas Spencer		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Negative	Comments Submitted
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Third-Party Comments
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	Scott Hoggatt		Negative	Third-Party Comments
6	Westar Energy	Megan Wagner		Negative	Third-Party Comments
6	Xcel Energy, Inc.	Carrie Dixon		Negative	Third-Party Comments
7	Exxon Mobil	Jay Barnett		Negative	Comments Submitted
7	Luminant Mining Company LLC	Stewart Rake		Negative	Comments Submitted
7	Oxy - Occidental Chemical	Venona Greaff		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Third-Party Comments
8	Foundation for Resilient Societies	William Harris		Negative	Comments Submitted
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Negative	Comments Submitted
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 373 of 373 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/80)
Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 Non-binding Poll IN 1 NB
Voting Start Date: 2/24/2017 12:01:00 AM
Voting End Date: 3/6/2017 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 289
Total Ballot Pool: 351
Quorum: 82.34
Weighted Segment Value: 10.88

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	89	1	7	0.121	51	0.879	14	17
Segment: 2	7	0.5	0	0	5	0.5	2	0
Segment: 3	80	1	4	0.069	54	0.931	11	11
Segment: 4	22	1	1	0.063	15	0.938	2	4
Segment: 5	81	1	6	0.12	44	0.88	11	20
Segment: 6	56	1	6	0.143	36	0.857	6	8
Segment: 7	3	0.2	0	0	2	0.2	1	0
Segment: 8	4	0.3	1	0.1	2	0.2	0	1
Segment: 9	1	0	0	0	0	0	1	0
Segment: 10	8	0.5	1	0.1	4	0.4	2	1
Total	351	6.5	26	0.715	213	5.785	50	62

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Negative	Comments Submitted
1	Austin Energy	Thomas Standifur		Negative	Comments Submitted
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Negative	Comments Submitted
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Negative	Comments Submitted
1	Basin Electric Power Cooperative	David Rudolph		Negative	Comments Submitted
1	BC Hydro and Power Authority	Patricia Robertson		None	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	Comments Submitted
1	Bonneville Power Administration	Kammy Rogers-Holliday		Negative	Comments Submitted
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		Negative	Comments Submitted
1	CMS Energy - Consumers Energy Company	James Anderson		None	N/A
1	Colorado Springs Utilities	Devin Elverdi		Negative	Comments Submitted
1	Con Ed - Consolidated Edison Co. of New York	Kelly Silver		Negative	Comments Submitted
1	CPS Energy	Glenn Pressler		Negative	Comments Submitted
1	Dairyland Power Cooperative	Robert Roddy		Abstain	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Negative	Comments Submitted
1	El Paso Electric Company	Pablo Onate		Negative	Comments Submitted
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Negative	Comments Submitted
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Aubrey Short		Negative	Comments Submitted
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Negative	Comments Submitted
1	Great River Energy	Gordon Pietsch		Negative	Comments Submitted
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Abstain	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Negative	Comments Submitted
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Negative	Comments Submitted
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Negative	Comments Submitted
1	JEA	Ted Hobson	Joe McClung	Negative	Comments Submitted
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		None	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Negative	Comments Submitted
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Negative	Comments Submitted
1	Memphis Light, Gas and Water Division	Allan Long		None	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Negative	Comments Submitted
1	National Grid USA	Michael Jones		Negative	Comments Submitted
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	Comments Submitted
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Negative	Comments Submitted
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Negative	Comments Submitted
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Negative	Comments Submitted
1	OTP - Otter Tail Power Company	Charles Wicklund		Negative	Comments Submitted
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Abstain	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 1 of Snohomish County	Long Duong		Negative	Comments Submitted
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		Abstain	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Negative	Comments Submitted
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Negative	Comments Submitted
1	Salt River Project	Steven Cobb		Negative	Comments Submitted
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Negative	Comments Submitted
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	Negative	Comments Submitted
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Negative	Comments Submitted
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		None	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Negative	Comments Submitted
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Negative	Comments Submitted
1	Tennessee Valley Authority	Howell Scott		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tri-State G and T Association, Inc.	Tracy Sliman		Negative	Comments Submitted
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Negative	Comments Submitted
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Negative	Comments Submitted
2	ISO New England, Inc.	Michael Puscas		Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Negative	Comments Submitted
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Negative	Comments Submitted
3	Austin Energy	W. Dwayne Preston		Negative	Third-Party Comments
3	Avista - Avista Corporation	Scott Kinney		Negative	Comments Submitted
3	Basin Electric Power Cooperative	Jeremy Voll		Negative	Comments Submitted
3	BC Hydro and Power Authority	Faramarz Amjadi		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Dehn Stevens	Darnez Gresham	Negative	Comments Submitted
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Negative	Comments Submitted
3	Bonneville Power Administration	Rebecca Berdahl		Negative	Comments Submitted
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Negative	Comments Submitted
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	Comments Submitted
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	Comments Submitted
3	City Utilities of Springfield, Missouri	Scott Williams		Negative	Comments Submitted
3	Clark Public Utilities	Jack Stamper		None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Abstain	N/A
3	Colorado Springs Utilities	Hillary Dobson		Negative	Comments Submitted
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Negative	Comments Submitted
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		Negative	Comments Submitted
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Negative	Comments Submitted
3	El Paso Electric Company	Rhonda Bryant		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Eversource Energy	Mark Kenny		Negative	Comments Submitted
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Negative	Comments Submitted
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	Comments Submitted
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	Comments Submitted
3	Georgia System Operations Corporation	Scott McGough		Negative	Comments Submitted
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Negative	Comments Submitted
3	Great River Energy	Brian Glover		Negative	Comments Submitted
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Abstain	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		None	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Negative	Comments Submitted
3	Manitoba Hydro	Karim Abdel-Hadi		Affirmative	N/A
3	MEAG Power	Roger Brand	Scott Miller	Negative	Comments Submitted
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Negative	Comments Submitted
3	National Grid USA	Brian Shanahan		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Negative	Comments Submitted
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Negative	Comments Submitted
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Negative	Comments Submitted
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Negative	Comments Submitted
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Negative	Comments Submitted
3	Ocala Utility Services	Randy Hahn		Negative	Comments Submitted
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Negative	Comments Submitted
3	Omaha Public Power District	Aaron Smith		Negative	Comments Submitted
3	Orlando Utilities Commission	Ballard Mutters		Negative	Comments Submitted
3	OTP - Otter Tail Power Company	Wendi Olson		Negative	Comments Submitted
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Negative	Comments Submitted
3	Platte River Power Authority	Jeff Landis		Negative	Comments Submitted
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Negative	Comments Submitted
3	Salt River Project	Rudy Navarro		Negative	Comments Submitted
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		Negative	Comments Submitted
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Daniel Frank	Negative	Comments Submitted
3	Sho-Me Power Electric Cooperative	Jeff Neas		None	N/A
3	Snohomish County PUD No. 1	Mark Oens		Negative	Comments Submitted
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		Negative	Comments Submitted
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Negative	Comments Submitted
3	TECO - Tampa Electric Co.	Ronald Donahey		Negative	Comments Submitted
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Negative	Comments Submitted
3	Westar Energy	Bo Jones		Negative	Comments Submitted
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Austin Energy	Tina Garvey		Negative	Third-Party Comments
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	Comments Submitted
4	City Utilities of Springfield, Missouri	John Allen		Abstain	N/A
4	CMS Energy - Consumers Energy Company	Beth Fields		None	N/A
4	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Negative	Comments Submitted
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	Comments Submitted
4	Georgia System Operations Corporation	Guy Andrews		Negative	Comments Submitted
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Negative	Comments Submitted
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Negative	Comments Submitted
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Negative	Comments Submitted
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Negative	Comments Submitted
4	Utility Services, Inc.	Brian Evans-Mongeon		Negative	Comments Submitted
4	WEC Energy Group, Inc.	Anthony Jankowski		Negative	Comments Submitted
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Negative	Comments Submitted
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Negative	Comments Submitted
5	BC Hydro and Power Authority	Helen Hamilton Harding		None	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock	Jeffrey Watkins	Negative	Comments Submitted
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	Comments Submitted
5	Bonneville Power Administration	Francis Halpin		Negative	Comments Submitted
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		Negative	Comments Submitted
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Abstain	N/A
5	Colorado Springs Utilities	Jeff Icke		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Con Ed - Consolidated Edison Co. of New York	Brian O'Boyle		Negative	Comments Submitted
5	CPS Energy	Robert Stevens		Negative	Comments Submitted
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Randi Heise		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		Negative	Comments Submitted
5	Duke Energy	Dale Goodwine		Negative	Comments Submitted
5	Edison International - Southern California Edison Company	Thomas Rafferty		None	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	El Paso Electric Company	Victor Garzon		Negative	Comments Submitted
5	Eversource Energy	Timothy Reyher		Negative	Comments Submitted
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Negative	Comments Submitted
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	Comments Submitted
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Negative	Comments Submitted
5	Great River Energy	Preston Walsh		Negative	Comments Submitted
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		None	N/A
5	JEA	John Babik		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Kissimmee Utility Authority	Mike Blough		Negative	Comments Submitted
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		Abstain	N/A
5	Lower Colorado River Authority	Wesley Maurer		Negative	Comments Submitted
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Abstain	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Negative	Comments Submitted
5	Muscatine Power and Water	Mike Avesing		Negative	Comments Submitted
5	National Grid USA	Elizabeth Spivak		None	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Erick Barrios		Negative	Comments Submitted
5	NextEra Energy	Allen Schriver		Abstain	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Negative	Comments Submitted
5	Northern California Power Agency	Marty Hostler		Negative	Comments Submitted
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		Negative	Comments Submitted
5	Omaha Public Power District	Mahmood Safi		Negative	Comments Submitted
5	Ontario Power Generation Inc.	David Ramkalawan		Abstain	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Negative	Comments Submitted
5	Portland General Electric Co.	Ryan Olson		None	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		None	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Negative	Comments Submitted
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		Negative	Comments Submitted
5	Puget Sound Energy, Inc.	Eleanor Ewry		None	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Negative	Comments Submitted
5	Salt River Project	Kevin Nielsen		Negative	Comments Submitted
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Negative	Comments Submitted
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		Negative	Comments Submitted
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Negative	Comments Submitted
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	None	N/A
5	SunPower	Bradley Collard		None	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		None	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Negative	Comments Submitted
5	Tennessee Valley Authority	M Lee Thomas		Negative	Comments Submitted
5	Tri-State G and T Association, Inc.	Mark Stein		None	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		None	N/A
6	AEP - AEP Marketing	Dan Ewing		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		None	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Negative	Comments Submitted
6	Austin Energy	Andrew Gallo		Negative	Comments Submitted
6	Basin Electric Power Cooperative	Paul Huettl		Negative	Comments Submitted
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Negative	Comments Submitted
6	Black Hills Corporation	Eric Scherr		Negative	Comments Submitted
6	Bonneville Power Administration	Andrew Meyers		Negative	Comments Submitted
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Colorado Springs Utilities	Shannon Fair		Negative	Comments Submitted
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Negative	Comments Submitted
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Negative	Comments Submitted
6	El Paso Electric Company	Luis Rodriguez		Negative	Comments Submitted
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Negative	Comments Submitted
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	Comments Submitted
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	Comments Submitted
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Negative	Comments Submitted
6	Great River Energy	Donna Stephenson	Michael Brytowski	Negative	Comments Submitted
6	Lakeland Electric	Paul Shipps		Negative	Comments Submitted
6	Lincoln Electric System	Eric Ruskamp		Abstain	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Negative	Comments Submitted
6	Lower Colorado River Authority	Michael Shaw		None	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Ryan Streck		Negative	Comments Submitted
6	New York Power Authority	Shivaz Chopra		Negative	Comments Submitted
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Negative	Comments Submitted
6	Northern California Power Agency	Dennis Sismaet		Negative	Comments Submitted
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Negative	Comments Submitted
6	Omaha Public Power District	Joel Robles		Negative	Comments Submitted
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Daniel Mason		Abstain	N/A
6	Powerex Corporation	Gordon Dobson-Mack		None	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		None	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Negative	Comments Submitted
6	Salt River Project	Bobby Olsen		Negative	Comments Submitted
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Negative	Third-Party Comments
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		Negative	Comments Submitted
6	TECO - Tampa Electric Co.	Benjamin Smith		Negative	Comments Submitted
6	Tennessee Valley Authority	Marjorie Parsons		Negative	Comments Submitted
6	WEC Energy Group, Inc.	Scott Hoggatt		Negative	Comments Submitted
6	Westar Energy	Megan Wagner		Negative	Comments Submitted
7	Exxon Mobil	Jay Barnett		Negative	Comments Submitted
7	Luminant Mining Company LLC	Stewart Rake		Abstain	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Negative	Comments Submitted
8	David Kiguel	David Kiguel		Negative	Comments Submitted
8	Foundation for Resilient Societies	William Harris		Negative	Comments Submitted
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		None	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Florida Reliability Coordinating Council	Peter Heidrich		Abstain	N/A
10	Midwest Reliability Organization	Russel Mountjoy		None	N/A
10	New York State Reliability Council	ALAN ADAMSON		Negative	Comments Submitted
10	Northeast Power Coordinating Council	Guy V. Zito		Negative	Comments Submitted
10	ReliabilityFirst	Anthony Jablonski		Negative	Comments Submitted
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Negative	Comments Submitted

Previous 1 Next

Showing 1 to 351 of 351 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1

Formal Comment Period Open through March 6, 2017
Ballot Pools Forming through February 17, 2017

Now Available

A 45-day formal comment period for **CIP-013-1 - Cyber Security – Supply Chain Risk Management**, is open through **8 p.m. Eastern, Monday, March 6, 2017**.

Commenting

Use the electronic form to submit comments on the standard. If you experience any difficulties in using the electronic form, contact Nasheema Santos. An unofficial Word version of the comment form is posted on the project page.

Join the Ballot Pools

Ballot pools are being formed through **8 p.m. Eastern, Friday, February 17, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for the standard and non-binding poll of the associated Violation Risk Factors and Violation Severity Levels will be conducted **February 24 – March 6, 2017**.

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

For more information or assistance, contact Senior Standards Developer, Mark Olson (via email) or at (404) 446-9760.

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

Comment Report

Project Name:	2016-03 Cyber Security Supply Chain Risk Management | CIP-013-1
Comment Period Start Date:	1/19/2017
Comment Period End Date:	3/6/2017
Associated Ballots:	2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 Non-binding Poll IN 1 NB

There were 134 sets of responses, including comments from approximately 231 different people from approximately 144 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

9. Provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC
					Jeffrey Partington	Keys Energy Services	4	FRCC

					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Joe McClung	Joe McClung		FRCC	JEA Voters	Ted Hobson	JEA	1	FRCC
					Garry Baker	JEA	3	FRCC
					John Babik	JEA	5	FRCC
MGE Energy - Madison Gas	Joseph DePoorter	4		MRO NSRF	Joseph DePoorter	MGE	1,2,3,4,5,6	MRO

and Electric Co.					Joseph DePoorter	MGE	1,2,3,4,5,6	MRO
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Con Ed - Consolidated Edison Co. of New York	Kelly Silver	1	NPCC	Con Edison	Kelly Silver	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange and Rockland Utilities	NA - Not Applicable	NPCC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and NextEra	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC

					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	UI	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					MIchael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Greg Campoli	NY-ISO	2	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
					Quintin Lee	Eversource Energy	1	NPCC
Colorado Springs Utilities	Shannon Fair	6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC

					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Gray	Board of Public Utilities,KS (BPU)	3	SPP RE
					Shawn Eck	Empire District Electric Company	1,3,5	SPP RE
Santee Cooper	Shawn Abrams	1		Santee Cooper	Tom Abrams	Santee Cooper	1	SERC
					Rene' Free	Santee Cooper	1	SERC
					Bob Rhett	Santee Cooper	5	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
PPL NERC Registered Affiliates	Shelby Wade	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Charlie Freibert	LG&E and KU Energy, LLC	3	SERC
					Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Dan Wilson	LG&E and KU Energy, LLC	5	SERC
					Linn Oelker	LG&E and KU Energy, LLC	6	SERC
Public Service Enterprise	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF

Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF
Midcontinent ISO, Inc.	Terry BIlke	2		IRC-SRC	Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

As stated in FERC Order 829, section 59, “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”. R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59.

If Future is added, the NSRF request that “Future” needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then the NSRF request a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.

The SDT should update R1 to clearly state this, such as;

“R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts concerning the procurement of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: “

This proposed update aligns with FEERC Order 829, section 59 and clearly informs the applicable entity in what is required in future endeavors. R1 will fulfill the FERC directive of having supply chain risk management plans for future procurement, which falls in line with the SDT’s “Notional BES Cyber System Life cycle” model. The NSRF does not agree with the “if applicable” wording and the addition of :” associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets”, as this is not within the FERC Order.

R1.1 and its parts seem to be disjointed. The NSRF understands to have a Plan (R1) to mitigate cyber security risks to the future procurement of BES Cyber Systems, etc. Within the Plan, entities are to use controls in **their** BES Cyber System planning and development “phase” (which is taken as the Entity’s internal processes of wants and needs). To have controls during the “planning and development” phase will not have an impact on the

procurement of a BES Cyber System, etc., since nothing is occurring; this is a planning phase, only. Entities are only discussing their wants and needs. This is similar to the caveat within the NERC Defined term of Operating Instruction; (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.) R1.1 has two parts that should address what is required to occur within the plan concerning the objective of R1.1.

Recommend R1.1 to read “The use of controls for BES Cyber Systems to:”

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services; and” (unchanged for the proposed draft). This updated wording of R1.1, directs the use of controls within the plan of R1 and R1.1 states use controls to accomplish the attributes of R1.1.1.

Then R1.1.2, states the Entity is to “…**evaluate methods to address** identified risk(s)”. As written, the Entity is to review (address?) their **methods** to mitigate identified risk(s). Without saying, does this part need to be within the proposed Standard? The intent is to mitigate any known risks, not evaluate **methods** to identify risk(s). This could be viewed as an entity’s **method** of industry trends to see what new “processes” there are to “evaluate methods to address identified risk(s). Or is this required in order to keep the “how and what” an entity does up to date and current with known “identify and assess” practices. If so, please clarify.

It may be less ambiguous if R1.1.2 is rewritten to read; “Evaluate mitigation methods to address identified risk(s)”. This clearly supports R1 where the Requirement states “…controls for mitigating cyber security risks…”.

Request that R1.2.parts be updated so Entities will clearly know their expectations under this proposed Standard:

R1.2.1, Process(es) for receiving notification of vendor identified security events; or “Process(es) for receiving notification and release notes of vendor identified security events;

Justification: this updated wording will establish agreed upon processes between the vendor and entity.

R1.2.2, Process(es) for being notified cation when vendor employee remote or onsite access should no longer be granted;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and that the entity need to be kept current on who is authorized by the vendor and allowed by the entity to access BES Cyber Systems.

1.2.3, Process(es) for disclosure of known applicable system vulnerabilities;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and not present a catch 22 when a vendor does not share applicable system vulnerabilities. We also request the “applicable system” be added (as above). Entities may have other vulnerabilities that will not impact the entity’s applicable system.

1.2.4, Coordination of response to vendor-related cyber security incidents;

No change.

1.2.5. Process(es) for verifying software integrity and authenticity of all applicable software and patches that are intended for use;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and relates R1.2.3 since the vendor disclosed a vulnerability. Suggest rewording to ensure that it only applies to situations where the vendor provides means to verify software, since standard does not impose requirements on vendors, Responsible Entity would otherwise be forced into non-compliance.

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

No change.

1.2.7. Other pProcess(es) to address risk(s) as determined in Part 1.1.2, if applicable.

Justification: The use of the word “other” is too broad based and could be viewed as all processes, even those outside of the NERC arena. With the clause of “... in Part 1.1.2, if applicable” clearly points to the identified risks of R1.1.2.

Within R1, R1.2, the SDT added the clause, “if applicable” as it relates to EACMS, PACS and PCA’s and the NSRF has concerns with this. As written in the proposed Standard’s rational box, this item is covered in P.59. FERC Order 829, P. 59, in part states:

“59. 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”.

FERC does not state the use of EACMS, PACS and PCA’s, but rather “…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” (emphasis added).

By the SDT interpreting P 59 to mean EACMS, PACS and PCA’s, this unnecessarily expands the scope of this proposed Standard above and beyond the FERC directive. The NSRF views this as, 1) future contracts concerning security concepts and 2) that support BES operations, which is the BES Cyber Systems identified per CIP-002-5.1a, only. Notwithstanding that EACMAS and PACS is not associated with Low impact BES Cyber Systems. Recommend that R1 and R1.2 have the “if applicable, EACMS, PACS and PCA’s” clause deleted. This will allow the Responsible Entity to have their own risk based controls within their supply chain risk management plan(s) based on the definition of BES Cyber System.

Additional NSRF concerns:

The following statement is taken directly from the Rationale for Requirement R1: "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This, in our opinion, is not conveyed in the written standard's requirement. Though vendors are not intended to be affected by this standard's requirements, Registered Entities will be forced to shy away from purchasing software from companies that cannot meet this standard. We see Regional Entities' Enforcement teams having a difficult time in upholding any possible violations with this standard.

R1. Comments

When it states "if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" what is their intent with the word applicable? It should either be applied or not applied to the systems. If the intent is to give the decision to the Registered Entities make this clearer, or remove the non-BCSs, completely.

R1.1.2 Comments

Add "mitigation" to methods. The intent is to alleviate an identified assessed risk.

Likes 2	Platte River Power Authority, 5, Archie Tyson; OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

- Recommend rewording Requirement 1 to: "Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control

or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets, ***to specifically address the risk of introduction of malicious code through the supply-chain process.*** The plan(s) shall address:" This addition clearly scopes the plan without relying on the title alone to hint at the proper scope.

- Is 1.1.2 only evaluating or is it evaluating and implementing?

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

The expressions, “Identify and assess risk(s),” in R1.1.1 and, “Evaluate methods to address identified risk(s),” in R1.1.2 are unsuitably vague.

TFE opportunity is needed, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses).

Terms such as, “vendor security event,” should be defined or removed.

R1.2.2 conflicts with CIP-004-6 R5 and should therefore be deleted.

R1.2.5 is largely duplicative of R3 and R5 of the standard. They should be made consistent, or one of them should be deleted.

R1.2.6 is largely duplicative of R4 of the standard. They should be made consistent, or one of them should be deleted.

The R1 Rationale statement that CIP-013-1, “does not require the Responsible Entity to renegotiate or abrogate existing contracts,” implies that no action needs to be taken for existing PEDs. This point should be made explicit in the standard per se, but our “additional comments” concerns would still apply for replacing or upgrading existing equipment.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John

Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	

R1 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R1 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R1 should be rewritten to be only applicable to high and medium impact BES Cyber Systems

Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

Requirement 1 should state specifically, as to its purpose, to prevent the introduction of malware or malicious code through the supply-chain process.

There should be an official NERC definition of the term ‘Vendor(s)’. Although the Rational and Guidelines for each define the term, there should be a more official definition in order to provide appropriate guidance for the auditors when evaluating compliance to this standard.

What does Requirement 1.1.2 mean? ... The plan(s) shall address: The use of controls … to: Evaluate methods to address identified risk(s). If a risk is identified during procurement and deployment, are we only required to evaluate methods to address those risks – or *address* the risks? This is incredibly confusing and leaves this requirement wide-open to interpretation.

The rational for Requirement R5 is identified as being based on FERC Order 829 (page 48), which specifically addresses Vendor Remote Access to BES Cyber Systems, without respect to applicability – Sections 76-80. Multiple requirements are referenced in Standards CIP-004, CIP-005 and CIP-007 that are only applicable to High and/or Medium Impact BESCS with weaknesses identified by not directly addressing vendor initiated machine-to-machine remote access. In the final sentence of Section 80, it is noted that vendor remote access is not adequately addressed in the ‘Approved’ standards and, therefore, is an objective that must be addressed in the supply chain management plans. Again, there is no reference to applicability, whereas the meat of the directive covers approved standards that reference Medium and High impact BESCS.

The scope and content of the already approved standards is the appropriate place to account for this weakness. A full impact and applicability analysis should be performed prior to proposed modification(s).

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Change/add language to emphasize that failure to obtain the cyber security controls from a vendor doesn't translate to being out of compliance. Entity should have the ability to mitigate risks posed by vendors. IID feels that the SDT should consider modifications to current CIP standards where the topic is already addressed.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

1. The standard lacks clarity on addressing R1.2 sub-requirements where no relationship of any sort exists between a RE and vendors whose products may be installed on applicable systems.

Many software and hardware components utilized on BES Cyber Systems, associated EACMS, PCA, and PACS systems are provided without any contractual agreement other than acceptance of a End-User-License-Agreement (EULA) upon installation.

For example, the Java Resource Environment, which is provided by Oracle Corporation, is utilized by many products. However, there is no agreement or financial transaction associated with the acquisition of Java.

This is even further complicated where open-source software is utilized for which no formal organization holds responsibility.

Finally, some proprietary software is acquired without any contractual arrangements due to low acquisition costs, such as an SSH client for less than $200.

In the case where there is a lack of relationship and/or financial interest in establishment of a formal agreement, how can RE address the provided requirements?

2. What incentive does a vendor have to disclose their vulnerabilities to a client? Wouldn't this disclosure ultimately serve to publicize the vulnerabilities?

Responsible entities can request this cooperation, but verification that the vendor is disclosing all vulnerabilities is not possible.

Likes 0	
Dislikes 0	

Response

Eric Ruskamp - Lincoln Electric System - 6

Answer	No
Document Name	

Comment

During the CIP-013-1 webinar on Feb 2, the SDT indicated several times that it is not the intention of R1 to force vendors to perform actions so that entities can comply with the standard. R1.2.1, R1.2.2, R1.2.3 would force vendors to develop internal processes to notify entities of any changes relating to the requirements which would force vendors to take independent action to notify entities of any changes. Also, during the procurement phase, why would vendors reveal potential security flaws in their product above and beyond normal security patch notifications while they are competing against other vendors for the entities business? This seems like wishful thinking. Also, entities have processes in place already for other CIP requirements to fully prepare an asset for deployment into the ESP. We don't grab equipment off of the back of the delivery truck and deploy it into the ESP immediately so what is the point of knowing about security flaws in their products during procurement? Any security flaws are probably already addressed with patches that will be downloaded and installed when preparing the asset for deployment. Also, a vulnerability assessment has to be performed against the asset and CIP-007/CIP-005 security controls have to be checked prior to deployment. 1.2.1, 1.2.3, 1.2.4 appear to be redundant with CIP-007 R2 security patch management. Is the SDT expecting vendors to provide information about security/design flaws above and beyond the normal security patch notifications? If so, what kind of information would that be?

1.2.5 is troublesome as well (and it seems to be a duplicate of R3). Entities typically use update or proxy servers to discover and identify applicable security patches. For example, we use Windows Update Server Services to identify patches and roll them out once testing and approvals are complete. Do we need to check the check sums of the identified patches or can we trust that the update servers are authenticating the software?

Likes 0	
Dislikes 0	

Response

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SCE agrees with this requirement in concept. However, as written, this requirement contains several issues that SCE believes should be resolved. The language of CIP-013-1 Requirement R1 does not clearly state what is required and is open to several interpretations. For example, Requirement R1, 1.1 requires the use of controls to identify and assess risks during the procurement and deployment of vendor products and services. However, consistent with the COSO framework, a risk methodology identifies and assesses risks, and controls are used to mitigate those identified risks. In addition, the requirement and its subparts do not define the security objective. This lack of clarity in the language of Requirement R1 may pose issues during audit. We recommend the following language to clarify the requirement consistent with intent of the FERC Order No. 829 directives:

R1. Each Responsible Entity shall define, document, and implement one or more supply chain risk management methodologies(s) that address objectives, risks, and controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The defined methodologies(s) shall define controls used to mitigate the risks of entering into contracts with vendors who pose significant risks to responsible entity's information systems, of procuring products that fail to meet minimum security criteria, and of failing to receive adequate notice from compromised vendors, and shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

1.1 The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:

1.1.1 Process(es) for notification of vendor security events;

1.1.2 Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.1.3 Process(es) for disclosure of known vulnerabilities;

1.1.4 Coordination of response to vendor-related cyber security incidents;

1.1.5 Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

1.1.6 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

1.1.7 Other process(es) to address risk(s) as determined, if applicable.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy requests further clarification from the drafting team on R1 and whether it applies to Low impact BES Cyber Assets. Since the current language of the requirement is silent on the level of applicability, an entity may assume that R1 applies to all High, Medium, and Low Impact BES Cyber

Systems. Duke Energy disagrees with the concept of applying R1 to Low Impact BES Cyber Systems. At the outset, Low Impact BES Cyber Systems have been subject to a risk assessment and classified as Low Impact since they pose a minimal threat to the BES. Also, a Responsible Entity is not obligated to have an inventory list of its Low Impact BES Cyber Systems. In the rationale section of R5, it is even mentioned that a list of Low Impact BES Cyber Assets is not required. Without a list of Low Impact BES Cyber Systems, we fail to see how a Responsible Entity could demonstrate compliance with R1. For this reason, coupled with the fact that the Low Impact BES Cyber Systems pose a minimal risk to the BES, we do not believe R1 should be applicable to Low Impact BES Cyber Systems, and the requirement language should reflect the applicability.

Duke Energy requests confirmation that the rationale provided in R1 (and throughout the standard) be included in the standard, even after the standard has been finalized and approved. We feel that some of the language in the rationale is very useful, and that some of the language is warranted in the requirement(s) themselves. Specifically, the phrase used in the rationale of R1:

"Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

We feel that this language is significant enough as it pertains to R1.2 and the possibility of disagreement between an Entity and an external party, that it should be placed somewhere in the standard.

Lastly, we recommend the drafting team consider developing this standard similarly to CIP-002-5.1a with regards to the leveraging of a bright-line model of risk assessment. This will ensure that entities are assessing risk consistently of their vendors and removes the potential disagreement in audit that a regulator finds that the entity's risk determination is incorrect based on a different set of subjective criteria. This was the justification needed to move from the risk-based assessment methodology (RBAM) in CIP Versions 1 – 3 to the bright-line criteria developed in CIP Version 5.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

We have four concerns with the proposed requirement.

First, CIP-013 should follow the other CIP Standards with respect to Low BES Cyber Assets. R1 should clearly exclude Low BES Cyber Assets and refer to R5 for those assets, and all requirements related to Low BES Cyber Systems should be consolidated into R5.

Second, we are concerned that the difference in wording between R 1.1 which refers only to BES Cyber Systems, and R1.2 which includes EACMS, PACS and PCAs, is confusing and can cause inconsistencies in implementation. R1.1, and subsequently R1.2, should be rewritten to help with this. Please consider the following suggestions:

From: *"1.1 The use of controls in BES Cyber System planning and development to:"*

To: *"1.1 The use of controls in planning and development to:"*

From: "*1.2 The use of controls in procuring vendor product(s) or service(s) that address the Following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:"*

To: *"1.2 The use of controls in procuring vendor product(s) or service(s):* "

Third, we believe that the term "cyber security incident" in R1.2.4 should be capitalized to be clear that it is to be interpreted as the NERC-defined term "Cyber Security Incident".

Fourth, for consistency and clarity, we request the term 'supply chain risk management' be 'supply chain cyber security risk management' throughout the standard and guidance.

Likes 2	PPL - Louisville Gas and Electric Co., 6, Oelker Linn; Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC comments.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AECI contends that R1 should be separated into two distinct requirements. R1 should be revised to require the Responsible Entity to develop and document supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems... The SDT should then develop an additional requirement (R2) to require the Responsible Entity to implement the documented supply chain risk management plan(s) documented in R1.

In addition to the comments above, AECI supports the following comments submitted by the MRO NRSF:

“As stated in FERC Order 829, section 59, “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”. R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59.

If Future is added, the NSRF request that “Future” needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then the NSRF request a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.”

Furthermore, AECI urges the SDT to use the supply chain definition from NIST Special Publication 800-53 Rev.4 that was identified in paragraph 32, footnote 61 in this requirement.

Likes 0	
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	No
Document Name	

Comment

CHPD has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment

Platte River Power Authority (PRPA) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

PRPA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, PRPA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify

systems, PRPA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required, low with a reduced set of requirements to address their lower risk, PRPA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

PRPA requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

PRPA is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see PRPA’s response to Question #9 for additional information on exceptions).

PRPA notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 PRPA requests changing the word *evaluate* to *determine.*

For R1.2.1 PRPA requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 PRPA requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. PRPA requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

Austin Energy (AE) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

AE does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, XXX requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, XXX believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, XXX requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

AE requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

AE is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see XXX’s response to Question #9 for additional information on exceptions).

AE notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 AE requests changing the word *evaluate* to *determine.*

For R1.2.1 AE requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 AE requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. AE requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 2	Austin Energy, 4, Garvey Tina; Austin Energy, 3, Preston W. Dwayne
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

1. The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined in the standard or added to the NERC Glossary of Terms and capitalized when used.
2. It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.
3. R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:“The entity must document its determination as to

what are the supply chain risks. Once this determination has been made and documented, the audit team's professional judgement cannot override the determination made by the Responsible Entity. "

4. For R1: This requirement requires both the development and the implementation of a plan. We recommend modifying this requirement into three steps which follows the CIP-014 structure – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline. The timeline should use fixed dates or intervals and not dates that are linked to the completion of other compliance activities
5. For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This should be incorporated into the Requirement itself.
6. For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list "planning, acquisition and deployment" and versions of these terms in the diagram. R1.1 uses "planning and development". The meaning of "development" has not been clarified and is not part of the process addressed by this standard. Suggest that "development" be clarified or removed.
7. The standard as written addresses Vendor Risk Management and no other supply chain risks such as sole source and international dependencies. Suggest changing the name, purpose, and other areas of the standard from supply chain" to "vendor".

8. For R1.1.2:

    i. We recommend changing *evaluate* to *Determine.* We also seek further clarification of the intent. As, written the requirement is ambiguous:

        a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

        b. to evaluate the effectiveness of mitigating that risk? or;

        c. is it meant to identify what controls you have to mitigate the risks you have?

    ii. The evaluation of methods is a administrative task and similar to other tasks removed from the NERC standards as part of the Paragraph 81 project.

9. For R1.2.1: The words "Security Event" are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then this should be an officially defined term either in the standard or in the NERC glossary. The s definition provided in the glossary is "any identified, threatened, attempted or successful breach of vendor's components, software or systems" and "that have potential adverse impacts to the availability or reliability of BES Cyber Systems" It is unclear if the second portion is meant to be part of the definition. Many cyber systems, like firewalls, are under constant threat and attempts to breach the systems security. Suggest replacing "vendor security event" with "identification of a new security vulnerability". Vendors may not be able to determine if a vulnerability "could have potential adverse impact to the availability or reliability of BES Cyber System". This clause would only be applicable in determining when an entity would notify a vendor.

10. For R1.2.1: Page 6, line 12 of the Guidance and Examples document list both notification of security events from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both types of notifications.

11. For R1.2.1: The requirement for the" process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document.

12. For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document The requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that "A failure of a vendor to follow a defined process is not a violation of this Requirement."

13. Page 6, line 12 of the guidance details the notification of the vendor by the entity. It is unclear that the R1.2.1 requires notification by the entity to the vendor as detail in the guidance document.

14. Recommend that “Security Event” be changed to require the reporting of only newly identified security vulnerabilities.

15. Change 1.2.7 from pointing to 1.1.2 to 1.1.1. Remove 1.2 since 1.2.7 covers 1.2.

16. Do not agree with the current draft language that includes all High, Medium and Low BES Cyber Systems in Requirement R1. Suggests limiting this requirement to High and Medium only as the current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. If controls are needed for low impact, suggest moving these to R5 to consolidate all low impact into a single requirement.

17. The SDT needs to make sure that there is no duplication in the standards. Provide guidance on how areas that seem to overlap like Interactive Remote Access and CIP-005.

18. Request the SDT to consider adding the following language from the rationale to the language of the standard “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

19. The Rationale for R1, it states that R1, P1.1 addresses P 56 of Order No. 829. P 56 calls for a risk assessment of the entities internal systems with this language “how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes”. R1, P1.1.1 calls for a risk assessment of the vendors systems with this language “procurement and deployment of vendor products and services.” The language in the order does not match the language in the standard and therefore suggest that the language be consistent to provide clarity.

20. There could be an impact of contract requirements on the ability of public utilities to piggyback on wide-area contracts such as those of National Association of State Procurement Officials (NASPO) Cooperative, Western States Contracting Alliance (WSCA), Washington State Department of Enterprise Service, and others. Recommend that a exclusion be permitted in the case of such contracts, which are important to provide flexibility and negotiating strength for public utilities throughout the country. Include language that provides an exclusion for contracts that are covered by other laws or regulations.

21. The requirement should not reference the word “mitigation”. Suggest that “mitigate” be replace with “address” as listed in R1.2.

22. Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

Public Utility District No. 1 of Chelan County (CHPD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No
Document Name	

Comment

The Public Utility District No. 1 of Chelan County (CHPD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk

electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	No
Document Name	

Comment

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	
Comment	

R1.1 The lack of guidelines and technical basis within a balloted and approved standard itself (not in a separate document) will result in many different interpretations and expectations on how to meet the requirement. As demonstrated in the measures section, the section lacks specificity as potentially every correspondence with a vendor is subject to data request and audit.

Who is the vendor? Is it the manufacturer/software company, the reseller the hardware/software is acquired from, the shipping company, the integrator, others? For temporary staff, is the contract employee a vendor? These are just example questions.

A lack of guidelines and technical basis within the standard itself could result in a broad interpretation of R1.1 that provides higher risk with little or no additional security. As entities will have to guess the auditor's interpretation, it increases the likelihood that a standard will be violated due to poor definition.

R1.2 This requirement should define a specific minimum security standard in a manner that avoids the inefficiencies from hundreds of entities performing the same analysis. This inefficiency adds costs to entities and to vendors for items that will be passed on to entities. As written, only concepts are presented, not a minimum specification that entities and vendors can effectively use to cost effectively demonstrate compliance in a consistent manner across the industry.

Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	
Comment	

We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	
Response	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	
Comment	

CHPD has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP has an active role on the CIP-013 SDT with an employee serving as a member of the team as well as our support staff who are participating in the SDT meetings. In addition, SRP has been engaging in dialogue with peers of trade associations such as LPPC to address the CIP-013 standard development activities.

SRP continues to be a strong supporter of efforts that ensure the security of the Bulk Electric System. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order, while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

SRP does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, SRP requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, SRP believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required for low impact assets, with a reduced set of requirements to address their lower risk, SRP requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

SRP requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

SRP is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see SRP’s response to Question #9 for additional information on exceptions).

SRP notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 SRP requests changing the word *evaluate* to *determine.*

For R1.2.1 SRP requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 SRP requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. SRP requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

No objections to R1.1. Although the actual language of R1.2 seems sound, how does this language in the R1 rationale section , "***For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan***" (Section B, p. 5) manage risks associated with Supply Chain Management vendors? Where is the incentive for an entity to actively pursue vendor negotiations to minimize risks during the procurement phase? Merely adding control elements to an RFP that are not subsequently incorporated through vendor negotiations into a product or Service Level Agreement [SLA] seems to be nothing more than an academic exercise. At a minimum, under the current rationale the entity should provide working documents (as described in M1) of the negotiations process to demonstrate compliance with R1.2?

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3

Answer	No
Document Name	

Comment

The following language from the rational box for Requirement R1 does not seem to incentivize an entity to actively pursue vendor negotiations to minimize risks during the procurement phase.

For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Merely adding control elements to an RFP that are not incorporated through vendor negotiations seems to be nothing more than an academic exercise. At a minimum, under the current rational, the entity should provide working documents of the negotiations process to demonstrate compliance with R1.2. Extending the initial review and update, as necessary

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4

Answer	No
Document Name	

Comment

- The extent of the "supply chain risk management plan" should be more clearly defined. The Requirement language goes beyond what is typically considered "supply chain" activities (i.e. activities involving the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer) and includes ongoing operational protections. The Standard should more clearly define what is meant by "supply chain" and limit the associated Requirement to mitigating the associated risks. All other operational related

protections should be addressed within the existing CIP Standard that already cover the related protections (e.g. remote access controls should be included in CIP-007 and not in a supply chain standard).

- The R1 Supply Chain Risk Management plan is applicable to BES Cyber Systems of all impact levels (and any associated EACMS, PACs, and PCAs). The following recommendations are provided:
    - The inclusion of Low Impact BES Cyber Systems in the scope of the Supply Chain Risk Management Plan should be reconsidered. The existing CIP-002-5.1 and CIP-003-6 only requires an entity to identify asset(s) containing Low Impact BCS and does not require a documented inventory of low impact BCS/BCA or even a documented list of system/asset types. The expectations of the Requirement would make it very difficult for an Entity to demonstrate compliance without a list of Low Impact BCS/BCA.
    - If after reconsideration it is still deemed necessary to include Low Impact BCS within the scope of the Supply Chain Risk Management Plan, the supply chain Requirement should be removed from CIP-013 and added to CIP-003 with the rest of the requirements that are applicable to Low Impact BCS. SDTs have made conscious decisions to keep all Requirements applicable to Low Impact BCS within the CIP-003 Standard and not have them sprinkled throughout all the CIP Standards. Additional time should be taken in developing the standard to remain consistent with this approach. (Note: Reference the CIP-003-7i draft CIP Standard related to low impact BES System Transient Cyber Assets.)
- For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months.
- Use of the “Notional BES Cyber System Life Cycle” model is problematic. Entities plan and assess future cyber systems, but acquire, configure, deploy, and maintain individual cyber assets.
- R1 – 1.2.1, 1.2.3, 1.2.4 references to vendor security events, vulnerabilities, and incidents are undefined and potentially overly broad. Auditors may not collectively or individually agree with an individual RE’s assessment of how these terms are defined and used within their R1 Plan.
- R1 – appears to overlap with parts of several existing CIP Standards, including: CIP-003-6 R2 Att. 1, Section 3; CIP-004-6 R4.1 - 4.4 and R5.1 - 5.5; CIP-005-5 R2.1 - 2.3; CIP-007-6 R2.1, R5.1, 5.5, 5.6, 5.7; and CIP-010-2 R1.1. Expanding the scope of these existing CIP programs with a new Standard could unintentionally disrupt or conflict with current security architectures and/or critical operations. FE recommends that the SDT consider making coordinated modifications to the scope and applicability of CIP-003, 004, 005, 007 and 010, at some future date, rather than extending existing requirements to a new Standard, i.e. CIP-013. FE suggests that the scope of the Supply Chain Standard include the administrative controls needed to address Order 829, and the operational and technical security controls remain in the existing CIP standards.
- Measures and Evidence – Since the R1 requires an entity to show that the plan has been implemented, M1 does not adequately describe the evidence required to demonstrate implementation of the plan, i.e. especially for technical sub-requirements. (For example the evidence that an entity has implemented, “1.2.1 Process(es) for notification of vendor security events,” would likely require a process map for how vendor notifications are received, processed and resolved. Additionally, an auditor would likely want a sample of actual dated notifications from several vendors with dated evidence of consistent action and resolution.) FE recommends that the SDT provide additional guidance on evidence types, formats etc… similar to what was provided in CIP-003-6 Attachment 2.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment
Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	

Comment
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	

Comment
R1, R2, and R5 contain obligations that apply to low impact BES Cyber Systems. With the inherent low risk that comes with these systems, Basin Electric questions whether the same protections for highs and mediums should be applicable to lows, especially in context of R1. Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013. Basin Electric is concerned the inclusion of lows will necessitate maintaining a list of low BES Cyber Systems and possibly a list of low BES Cyber Assets. As stated in FERC Order 829, section 59, “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”. R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59. If Future is added, Basin Electric requests that “Future” needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then Basin Electric requests a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.

The SDT should update R1 to clearly state this, such as:

"R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts concerning the procurement of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: "

This proposed update aligns with FERC Order 829, section 59 and clearly informs the applicable entity in what is required in future endeavors. R1 will fulfill the FERC directive of having supply chain risk management plans for future procurement, which falls in line with the SDT's "Notional BES Cyber System Life cycle" model. Basin Electric does not agree with the "if applicable" wording and the addition of :" associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets", as this is not within the FERC Order.

R1.1 and its parts seem to be disjointed. Basin Electric understands to have a Plan (R1) to mitigate cyber security risks to the future procurement of BES Cyber Systems, etc. Within the Plan, entities are to use controls in **their** BES Cyber System planning and development "phase" (which is taken as the Entity's internal processes of wants and needs). To have controls during the "planning and development" phase will not have an impact on the procurement of a BES Cyber System, etc., since nothing is occurring; this is a planning phase, only. Entities are only discussing their wants and needs. This is similar to the caveat within the NERC Defined term of Operating Instruction; (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.) R1.1 has two parts that should address what is required to occur within the plan concerning the objective of R1.1.

Recommend R1.1 to read "The use of controls for BES Cyber Systems to:"

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services; and" (unchanged for the proposed draft). This updated wording of R1.1, directs the use of controls within the plan of R1 and R1.1 states use controls to accomplish the attributes of R1.1.1.

Then R1.1.2, states the Entity is to "…**evaluate methods to address** identified risk(s)". As written, the Entity is to review (address?) their **methods** to mitigate identified risk(s). Without saying, does this part need to be within the proposed Standard? The intent is to mitigate any known risks, not evaluate **methods** to identify risk(s). This could be viewed as an entity's **method** of industry trends to see what new "processes" there are to "evaluate methods to address identified risk(s). Or is this required in order to keep the "how and what" an entity does up to date and current with known "identify and assess" practices. If so, please clarify.

It may be less ambiguous if R1.1.2 is rewritten to read; "Evaluate mitigation methods to address identified risk(s)". This clearly supports R1 where the Requirement states "…controls for mitigating cyber security risks…".

Request that R1.2.parts be updated so Entities will clearly know their expectations under this proposed Standard:

Please add clarification to what is meant by vendor “services” as stated in R1.2.

R1.2.1, Process(es) for receiving notification of vendor identified security events; or “Process(es) for receiving notification and release notes of vendor identified security events;

Justification: this updated wording will establish agreed upon processes between the vendor and entity.

R1.2.2, Process(es) for being notified when vendor employee remote or onsite access should no longer be granted;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and that the entity need to be kept current on who is authorized by the vendor and allowed by the entity to access BES Cyber Systems.

1.2.3, Process(es) for disclosure of known applicable system vulnerabilities;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and not present a catch 22 when a vendor does not share applicable system vulnerabilities. We also request the “applicable system” be added (as above). Entities may have other vulnerabilities that will not impact the entity’s applicable system.

1.2.5. Process(es) for verifying software integrity and authenticity of all applicable software and patches that are intended for use;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and relates R1.2.3 since the vendor disclosed a vulnerability. Suggest rewording to ensure that it only applies to situations where the vendor provides means to verify software, since standard does not impose requirements on vendors, Responsible Entity would otherwise be forced into non-compliance.

1.2.7. Process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

Justification: The use of the word “other” is too broad based and could be viewed as all processes, even those outside of the NERC arena. With the clause of “... in Part 1.1.2, if applicable” clearly points to the identified risks of R1.1.2.

Within R1, R1.2, the SDT added the clause, “if applicable” as it relates to EACMS, PACS and PCA’s and Basin Electric has concerns with this. As written in the proposed Standard’s rational box, this item is covered in P.59. FERC Order 829, P. 59, in part states:

“59. 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”.

FERC does not state the use of EACMS, PACS and PCA's, but rather "…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" (emphasis added).

By the SDT interpreting P 59 to mean EACMS, PACS and PCA's, this unnecessarily expands the scope of this proposed Standard above and beyond the FERC directive. Basin Electric views this as, 1) future contracts concerning security concepts and 2) that support BES operations, which is the BES Cyber Systems identified per CIP-002-5.1a, only. Notwithstanding that EACMAS and PACS is not associated with Low impact BES Cyber Systems. Recommend that R1 and R1.2 have the "if applicable, EACMS, PACS and PCA's" clause deleted. This will allow the Responsible Entity to have their own risk based controls within their supply chain risk management plan(s) based on the definition of BES Cyber System.

The following statement is taken directly from the Rationale for Requirement R1: "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This is not conveyed in the written standard's requirement. Though vendors are not intended to be affected by this standard's requirements, Registered Entities will be forced to shy away from purchasing software from companies that cannot meet this standard. We see Regional Entities' Enforcement teams having a difficult time in upholding any possible violations with this standard.

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

1.

   i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

   ii. To evaluate the effectiveness of mitigating that risk? or;

   iii. Is it meant to identify the controls in place to mitigate the identified risks?

Revise R1.2.1 as follows, "Process(es) for notification of vendor security events **that affect BES reliability**;"

For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

It is not clear if R1 applies to High, Medium and Low since R3, R4 and R5 specify the impact level. This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

R1.1 is vague in the language used with terms like “assess risk” and “evaluate”.

Concern that the Entity interpretation can be very different than Auditor interpretation. Once an entity has completed its risk evaluation, this determination cannot be overturned by the Regional Entity.

Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1

The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

- “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”
- “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment

See overview comments and comments specific to Req2uirement R1, in attached file.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	

Comment

Both the draft guidance document and the “Rationale for Requirement R1” section of the draft Standard contain the statement, “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” However, there is nothing in any Requirement or any Requirement Part containing such language. Language similar to existing technical feasibility language in CIP-002 through CIP-011 should be added.

N&ST considers requirement part 1.2.2 redundant with existing CIP-004-6 Requirements R4 and R5 and recommends that either it be deleted from this Standard or modified to indicate a Responsible Entity may address it with existing CIP-004 access management procedures.

N&ST considers requirement part 1.2.6 redundant with existing CIP-005-5 Requirements R1 and R2 and recommends that either it be deleted from this Standard or modified to indicate a Responsible Entity may address it with existing CIP-005 procedures for Electronic Access Points and for Interactive Remote Access.

N&ST also recommends that all “Vendor remote access” requirements relevant to supply chain management be presented in one top-level requirement, not in two (R1 and R4).

N&ST also recommends that all “Software integrity and authenticity” requirements be presented in one top-level requirement, not two (R1 and R3).

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment

We recommend the drafting team remove the phrase “if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets” from the language of Requirement R1 and Section 1.2 because, we feel that this language is inconsistent with FERC Order 829 Directive language. Also, we suggest that the drafting team add some clarity to the sub-parts of Section 1.2 so that the industry will clearly know their expectations.

In reference to Requirement R1 and contracts, we suggest that the term “future contracts” be included in the proposed language of the Requirement. Also, we suggest the drafting team develop a definition for the term “future contracts” that would potentially include the phrase “new or modified contracts on or after the date of Enforcement” in the proposed definition.

SPP’s proposed language revision to R1:

“Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts pertaining to the procurement of the BES Cyber System.”

Finally, we feel that the Measurement and Requirement language is inconsistent with the sub-part language. In the second sentence of the Requirement and Measurement the term “mitigating” is used, and we suggest replacing the term with “addressing”. We need to ensure all of our risk management options are available to us.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine [illegible]

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine ~~remote access~~ access.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?

1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.

1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?

1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?

Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We commend the drafting team for attempting to meet the directives and respect their effort and commitment to that end. We agree with now acting FERC chair LaFleur's comments in her dissent on Order 829, "The Commission is issuing a general directive in the Final Rule, in the hope that the standards team will do what the Commission clearly could not do: translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act."

We do not agree with the approach in R1 (and R2) of creating "plans" and the intent of the plans to "cover the procurement aspects of all four objectives."

Order 829's four objectives did not include creating "plans." All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011.

Standards will not be effective, auditable or enforceable with a CIP-013 standard dueling with CIP-002 through -011 on scope and obligations.

CIP-002 through -011 are the appropriate place to address these operational security controls. These standards establish the least ambiguity in scope of obligations. These standards make granular distinctions based on risk when assigning what BES Cyber Assets are subject to each requirement. The risk distinctions go beyond just low, medium or high impact and incorporate Control Center, External Routable Connectivity and Interactive Remote Access in assigning obligations for requirements.

NERC's Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets and all have very different risks to the grid and different obligations under CIP-002 through CIP-011.

"Plans" cannot achieve an effective, auditable and enforceable standard for 1,398 NERC entities that address the complicated issues identified in LaFleur's dissent … and certainly not to meet the September 2017 directed deadline.

Industry can at a minimum advance cyber security by revisions to operational security controls in CIP-002 through -011. Other commenters, including EEI, are submitting examples of language as starting points.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine machine remote ac

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Dominion supports the work that the drafting team has performed to-date and understands that the current draft of CIP-013-1 is continuing to evolve. Dominion has developed extensive comments to allow the drafting team to focus efforts on areas of particular concern with the current draft. Dominion supports the team's continued efforts to bring stakeholder knowledge and expertise together to develop an objective based reliability standard that realistically addresses reliability gaps in the cyber supply chain process.

- Dominion has a concern that the specific risks identified in P57 of FERC Order No. 829 are not included Requirement R1. The term used in the current draft of CIP-013-1, "cyber security risks", is overly broad and should be constrained by the enumerated risks in the FERC order.

Constraining language for the term 'cyber security risks' could include" risks associated with the of procurement and installation of unsecure equipment or software, the risks associated with unintentionally failing to anticipate security issues that may arise due to network architecture or during technology and vendor transitions, and the risks associated with purchasing software that is counterfeit or that has been modified by an unauthorized party."

Dominion recommends the development team consider the following language change for R1:

"Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that include security considerations related to cyber security risks related to procuring and installing unsecure equipment or software, the risk of unintentionally failing to anticipate security issues that may arise due to network architecture, unintentionally arise during technology and vendor transitions, and purchasing software that is counterfeit or that has been modified by an unauthorized party for BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets."

- In addition, Dominion recommends that system applicability should be clearly identified in the Rationale section of the requirement. Specifically, it is recommended that the "to the extent applicable" language should be removed from part 1. 2 and from the Rationale for R1.

- Dominion recommends the following for Parts 1.1.1 and 1.1.2:

    i. Identify and assess cyber security risk(s) to the BES, if any, during the procurement and deployment of vendor products and services; and

    ii. Evaluate methods to address identified risk(s).

- The term "services" in Part 1.2 is very broad and could be interpreted differently by different parties. To ensure consistent understanding of this term, Dominion recommends that the development team place context around the term 'service' as used in requirement R1.2 in a compliance guidance document.

- Dominion recommends that Part 1.2.7 be removed from CIP-013-1. The comprehensive list of risks in Parts 1.2.1 through 1.2.6 appropriately addresses the risk.

- As an alternative to the above recommendations, the development team could consider the following new proposed requirements in lieu of requirement R1 and R2:

R1: Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that include security considerations related to cyber security risks of 1) procuring and installing un-secure equipment or 2) procuring and installing un-secure software, including purchasing counterfeit software, or software that has been modified by an un-authorized party 3) unintentionally failing to anticipate security

issues that may arise due to network architecture, 4) unintentionally failing to anticipate security issues that may arise during technology and vendor transitions for BES Cyber Systems and associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The supply chain plan(s) shall address:

1. 1. Process(es) for notification of vendor security events;

1.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.3. Process(es) for disclosure by the vendor of known vulnerabilities;

1.4. Coordination of response to vendor-related cyber security incidents;

1.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use; and,

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

R2: The supply chain plan(s) shall include a process whereby any risk identified by the vendor during the purchasing process is assessed, reviewed, mitigating activities evaluated, and actions based on the selected mitigating activities implemented prior to placing the item(s) in service.

R3: The supply chain plan(s) shall be reviewed, updated as necessary, and approved by CIP SM or delegate at least once every fifteen (15) months.

The Rationale should explain that risks 1 and2 are addressed by R1.3 and R1.5, risk 3 by R1.1-R1.4 and R1.6, and risk 4 by R1.2, 1.3, and R1.6. And that the planning and system lifecycle processes are addressed in the order are expected to encapsulate the purchasing process and are covered by R2.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

In addition to high and medium impact BES Cyber Systems, the applicability of R1 should be clear to include low impact BES Cyber Systems.

SCE&G agrees with the concerns and question raised by the Security Practices Working Group of North American Generator Forum (NAGF) regarding "if applicable":

"The phrase "if applicable" is ambiguous in the language of the main requirement. One reading is that "if applicable" means that the requirement only applies should the device types of associated EACMS, PACS or PCAs actually exist. Another reading is that "if applicable" is based on the risk that an entity places on a particular vendor as part of its documented risk management plan(s). If an entity performs a risk assessment of its vendors and finds

that a vendor is a low or potentially zero risk (coupling a vendor's reputation with their particular usage within an entity), does this mean that an entity could determine that the protections in R1 are therefore "not applicable" and not place any additional expectations on them?"

SCE&G believes the current language of R1 places unacceptable burden on the Regional Entities because the obligations of R1 occur at the end of the supply chain between Regional Entity and its vendor(s). Cyber security risks can occur at any phase of the supply chain(s) and R1 does not clearly demarcate the supply chain(s) where the risk management plan(s) apply. It is not clear how far in the supply chain(s) of a BES Cyber Asset do Responsible Entities need to identify and assess procurement risks. SCE&G is concerned that Regional Entities will be held responsible for assessment and mitigation of risks outside of the Entities' realm of influence over vendor internal processes and vendor's supply chain(s).

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends that the overall structure of the proposed CIP-013 standard be changed to be consistent with CIP-004 through CIP-011 standards (Specifically by applying similar formatting and use of applicability tables to identify the in-scope systems.) NRG recommends that the CIP-013 standard should focus only on R1 and R2. This would allow the operational controls to remain or be placed in the existing CIP standards.

NRG suggests that the drafting team consider the risk impact classification for Requirement R1 as they would with the other Requirements through the Standard. Additionally, we suggest the drafting team remove the phrase "if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" from the language of R1 and section 1.2 because, we think that this language is inconsistent with FERC Order 829 Directive language. Also, we suggest that the drafting team adds some clarity to the sub-parts of Section 1.2 on what are the SDT intentions for the industry in reference to these sub-parts.

In reference to R1 and contracts, NRG suggests that the term "future contracts" be addressed in the requirement language such as: "new or modified contracts" on or after the date of Enforcement. NRG recommends that these terms should be vetted in an implementation plan to include a conversation of initial compliance versus implemented/ongoing compliance (for example, Registered Entities need clear understanding of the scope as it pertains to plan reviews, new contracts, modified contracts, current contracts).

The Measurement and Requirement language is inconsistent with the sub-part language. In the second sentence of R1's Measures section, the term "mitigating" is used and we suggest replacing the term with "addressing". NRG recommends that the term "addressing" includes that Registered Entities have the flexibility to exercise all risk management options within a Risk Management Plan (to include an acceptance of risk).

Each requirement should have a provision that allows an entity to accept the risk of selection a vendor that will not or cannot supply a control. The requirement intent appears to be about control of a process of disclosure and communication (how a vendor notifies us). Whether a vendor fixes a vulnerability does not appear to be the direct scope or intent of the requirement. Therefore, obtaining specific controls in the negotiated contract may not be feasible. In these cases, NRG suggests that a failure to obtain and implement these controls is not considered a failure to implement an entity's plan. NRG recommends that an entity be able to use a formalized risk management process to evaluate or accept the risk [Risk Management Plan]. In the event that a vendor cannot supply a control, that a Registered Entity may be able to present a mitigating control or that the Registered Entity be allowed to decide to accept the risk (for example a process to vet through a Registered Entity risk management, supply chain, and/or senior management departments and a process to accept risk based on a risk matrix). This may be implied by R1.2.7; however NRG recommends that the standard explicitly communicate that a level of risk acceptance can be part of an entities' Risk Management Plan. The Risk Management Plan could

include steps to keep track of failures and steps to take in the event that vendor controls are found to be insufficient (for example, lessons learned feedback and correction process) - in the Measures section. An example of demonstration of compliance could be a periodic (i.e. 15 month) survey to the vendor during plan review (i.e. 15 month) validation of the notification processes between the two parties or dependent on the level or risk. NRG recommends that R1 should have a description of elements of a good Risk Management Plan (Measures) to include how deficiencies will be addressed, regular feedback to the vendor, and potential implications of non-conformance. NRG requests clarity on how revisions to the Risk Management Plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

For R.1.2.7, NRG recommends using “or” vs “and” after R1.2.6

In R1.2, NRG recommends rewording the requirement to “implement processes that describe controls to address risks identified in R1.1.” NRG recommends that the intent of R1 to be to provide processes (for disclosure and responding controls). Therefore, NRG recommends that the Measure be limited to the sufficiency of the Entities’ vendor controls and evaluation process. The Measures should state that the evaluation would be on an entities process for evaluation and if a vendor does not uphold a negotiated communication process, this does not reflect a compliance violation on the Registered Entity.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined.

2. It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3. R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

4. For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5. For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6. For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list “planning, acquisition and deployment” and versions of these terms in the diagram. R1.1 uses “planning and development”. The meaning of “development” has not been clarified and is not part of the process addressed by this standard. Suggest that “development” be clarified or removed.

7. For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

    i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;
    ii. To evaluate the effectiveness of mitigating that risk? or;
    iii. Is it meant to identify the controls in place to mitigate the identified risks?

8. For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then” Security Event” should be replaced or clarified in the Requirement. This clarification could include “any identified, threatened, attempted or successful breach of the vendor’s components, software or systems used in the support of the Entity’s BES Cyber System.” This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3
9. For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.
10. For R1.2.2: The requirement for the” process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document the requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that “A failure of a vendor to follow a defined process is not a violation of this Requirement.”
11. Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk
12. Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1
13. The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

“Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

“Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

In addition to high and medium impact BES Cyber Systems, the applicability of R1 should be clear to include low impact BES Cyber Systems.

SCE&G agrees with the concerns and question raised by the Security Practices Working Group of North American Generator Forum (NAGF) regarding “if applicable”:

“The phrase “if applicable” is ambiguous in the language of the main requirement. One reading is that “if applicable” means that the requirement only applies should the device types of associated EACMS, PACS or PCAs actually exist. Another reading is that “if applicable” is based on the risk that an entity places on a particular vendor as part of its documented risk management plan(s). If an entity performs a risk assessment of its vendors and finds

that a vendor is a low or potentially zero risk (coupling a vendor's reputation with their particular usage within an entity), does this mean that an entity could determine that the protections in R1 are therefore "not applicable" and not place any additional expectations on them?"

SCE&G believes the current language of R1 places unacceptable burden on the Regional Entities because the obligations of R1 occur at the end of the supply chain between Regional Entity and its vendor(s). Cyber security risks can occur at any phase of the supply chain(s) and R1 does not clearly demarcate the supply chain(s) where the risk management plan(s) apply. It is not clear how far in the supply chain(s) of a BES Cyber Asset do Responsible Entities need to identify and assess procurement risks. SCE&G is concerned that Regional Entities will be held responsible for assessment and mitigation of risks outside of the Entities' realm of influence over vendor internal processes and vendor's supply chain(s).

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine machine remote ac

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined.

2) It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3) R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

4) For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5) For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6) For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list “planning, acquisition and deployment” and versions of these terms in the diagram. R1.1 uses “planning and development”. The meaning of “development” has not been clarified and is not part of the process addressed by this standard. Suggest that “development” be clarified or removed.

7) For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

{C}a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

{C}b. To evaluate the effectiveness of mitigating that risk? or;

{C}c. Is it meant to identify the controls in place to mitigate the identified risks?

8) For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then ”Security Event” should be replaced or clarified in the Requirement. This clarification could include “any identified, threatened, attempted or successful breach of the vendor’s components, software or systems used in the support of the Entity’s BES Cyber System.” This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3

9) For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

10) For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document The requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that “A failure of a vendor to follow a defined process is not a violation of this Requirement.”

11) Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

CenterPoint Energy believes requirement R1 should only be applicable to BES Cyber Systems and recommends removing the portion of the requirement in R1 and R1.2 that states “and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets”. The FERC order is focused on “industrial control system hardware, software, and services associated with bulk electric system operations” and does not mention Electronic Access Control and Monitoring System (EACMS), Physical Access Control System (PACS), or Protected Cyber Assets (PCA). These additional systems are low risk and not considered industrial control systems. CenterPoint Energy recommends taking a risk-based approach as stated in the FERC order, so entities can focus their efforts on the supply chain risk management of BES Cyber Systems, which pose a higher risk to the Bulk Electric System. Additionally, this requirement is applicable to High, Medium, and Low Impact BES Cyber Systems, but Low Impact BES Cyber Systems do not have EACMS, PACS, and PCA.

If the intent of R1 is address the procurement controls, CenterPoint Energy recommends stating that in the main R1 requirement; otherwise, the sub-requirements in R1 can appear to be duplicative of the technical operational controls in R3 and R4. Furthermore, the expectation for R1 is not clear for open source products with no vendor or products bought off the shelf with no purchase contract.

CenterPoint Energy recommends deleting R1.1.2 as the items in R1.2 appear to be the mitigation for the risks identified in R1.1. There is no need for a separate statement about mitigation in R1.1.2.

R1.2.1 uses the term “security events” which is not defined and the meaning could vary for each vendor. CenterPoint Energy recommends defining the term for consistency.

R1.2.2 appears to be redundant to CIP-004 R5.1 and R5.2 and extends to PACS and PCA requirements formerly required only for BES Cyber Systems (BCS) and Electronic Access Control and Monitoring Systems (EACMS).

R1.2.4 should capitalize the term “cyber security incident” because it is a NERC defined term.

R1.2.5 includes “all software and patches” which conflicts with the existing CIP Standards.

R1.2.6 is either redundant with or in conflict with CIP-005 requirements to identify inbound and outbound access permissions with reason for access and control remote access with 2 factor authentication and an identified access control system. It is unclear what additional evidence would be expected to satisfy this requirement.

R1.2.7 is far too broad, requiring and exposing to audit a potentially infinite number of new processes. The requirement wording is not appropriate for a Reliability Standard.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	No
Document Name	

Comment

OUC has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

OUC does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, OUC requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, OUC believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, OUC requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

OUC requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

OUC is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see OUC's response to Question #9 for additional information on exceptions).

OUC notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 OUC requests changing the word *evaluate* to *determine.*

For R1.2.1 OUC requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 OUC requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. OUC requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

At the main Requirement level, while the rationale for Requirement R1 clearly states,

"Implementation of the cyber security risk management plan(s) ***does not require*** *the Responsible Entity to renegotiate or abrogate* ***existing contracts****, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan",*

the requirement language is silent to this stipulation and therefore could lead to future confusion if left absent from the requirement language.

For ultimate clarity, ATC recommends the SDT consider the inclusion of language within the Requirement R1 itself that provides this specificity of scope. Proposed language for consideration could include phrasing like, but not limited to:

"Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) for ***new/future vendor/supply chain contracts, agreements, and/or relationships*** *that address controls for mitigating…"*

Additionally, it is not uncommon for operational technology to be proprietary, and as such to limit the supplier base and/or the industry's options/bargaining power over supplier practices. While the Rationale provided by the SDT carries the message that the intent is for this requirement to be forward-thinking and exclude existing contracts, even if the above proposed language were incorporated for clarity, it does not address the gap incurred after initial enforcement and implementation is achieved. Once the Standard would be enforceable, inevitably existing contracts will continue to age and will need to be renewed or renegotiated. This requirement language does not address that condition, the feasibility of the imposed obligations upon the future expiration of existing contracts, nor the potential unintended consequences that may be incurred at the time that renewal or renegotiation process are initiated as those existing contracts reach maturity and ultimately expiration. Consequently, the industry must assure that any future regulations regarding supply chain are constructed in a manner that 1.) supports successful and ongoing accomplishment of safe, secure,

resilient, and reliable operation of the Bulk Electric System as existing contracts reach maturity and inevitably age to the level of expiration, 2.) prevents the unintended consequences that are at variance with the intent to maintain safe, secure, resilient, and reliable operation of the Bulk Electric System.

As an example, some unintended consequences could include, and may not be limited to:

- Rendering previously contracted and necessary suppliers inviable upon the renewal or renegotiation of expiring/expired contracts creating a gap in the ability to procure necessary limited or proprietary supply that supports reliable operations,
- The industry being subject to the operationally risky, unnecessarily time-constrained, and cost prohibitive need to perform wholesale replacements of infrastructure with a new supplier to achieve compliance,
- The industry being held hostage by its suppliers through cost prohibitive supplier capitalization via unreasonable increase to the cost of supplier services containing contractual language that meet the CIP-013-1 requirements for their products/services.

The absence of a provision to accommodate for these potential conditions could lead to an impossibility of compliance and/or could compromise reliability if the Registered Entity 1.) cannot procure necessary products without being subject to a compliance violation, or 2.) is forced to abandon current solutions and perform wholesale upgrades or replacements of BES Cyber System infrastructure in order to comply, 3.) is forced to pay exorbitant fees to renegotiate/renew contracts with limited suppliers of necessary limited or proprietary products. Proposed language for consideration could include phrasing like, but not limited to:

"Each supply chain risk management plan(s) shall contain provisions to address instances where expired/expiring vendor/supply chain contracts, agreements, and/or relationships cannot be reasonably renewed in a compliant mode without posing significant risk to safe, secure, resilient, and reliable operation of the Bulk Electric System and its BES Cyber Assets."

Requirement R1:

The scope of R1 is too broad in its reference to BES Cyber Systems without consideration of impact-rating. Consequently, some of the proposed requirements are duplicative of existing requirements for high and/or medium impact BES Cyber Systems, and others exceed the controls required for approved and future enforceable CIP Cyber Security Reliability Standards for low impact BES Cyber Systems.

1. This approach is at odds with the overall intent for the CIP Cyber Security Standards to be constructed in a manner that applies graduated controls commensurate with the risk associated to the impact rating of the BES Cyber System.
2. This approach creates double jeopardy in certain instances, and is at variance with the approach to the body of documentation that comprises the CIP Cyber Security Standards wherein significant effort was invested to eliminate cross references and duplicative content.
3. Through it redundancy, this approach is at odds with the efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.
4. This approach is at odds with the directive in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard wherein "…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.

Requirement R1 Sub Requirement 1.1.2:

At the sub requirement level, R1 sub requirement 1.1.2 is broad and unclear. ATC recommends the SDT consider providing clarification if anything actionable is expected beyond just an evaluation, such as creating a plan to address the risk and then mitigating risk where possible.

Requirement R1 Sub Requirement 1.2.2:

R1.2.2 is simultaneously duplicative and additive to the language and/or intent of existing approved and effective CIP Cyber Security Reliability Standards as consequence of the broad reference to BES Cyber Systems without consideration of impact-rating in Requirement R1.

1. CIP-004-6 R4 and R5 address access management and revocation for **individuals** having cyber or unescorted access to specified high and/or medium impact-rated BES Cyber Systems and associated Cyber Assets. The existing enforceable CIP-004-6 standard is silent to the capacity with which a given individual is engaged with a Registered Entity, and therefore in its silence addresses employees, contractors, interns, apprentices, and even vendors or suppliers etc. The existing implemented access requirements within CIP-004-6 are more prescriptive than what is proposed for CIP-013-1 rendering CIP-013-1 R1.2.2 superfluous. Consequently, CIP-013-1 R1.2.2 adds no value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-004-6 R5. Through it redundancy, this approach is also at odds with the efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.

2. CIP-003-6 R1.2 prescribes policy level controls, and CIP-003-6 R2 Attachment 1 Sections 2-3 necessitate plans for the implementation of physical and electronic controls for low impact BES Cyber Systems. CIP-013-1 R1.2.2 effectively expands the scope and requirements for access of vendor employees beyond what is mandated as access requirements of low impact BES Cyber Systems to all other types of employees and Registered Entity engagements wit personnel. Any expansion in scope to access requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

3. Additionally, the inclusion of “onsite access” within the proposed language in 1.2.2 is an expansion in scope from the **second directive** in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard that “…should address the following security objectives, discussed in detail below: (1) software integrity and authenticity; **(2) vendor remote access**; (3) information system planning; and (4) vendor risk management and procurement controls.”

Requirement R1 Sub Requirement 1.2.4 and 1.2.6:

For consistency with other 1.2.x sub requirements, ATC recommends the SDT consider replacing ‘Coordination’ with ‘Process’ by revising the language in both R1.2.4 and R1.2.6 to “**Process** to respond to vendor-related….”, and “**Process** to implement remote access controls…”, respectively.

Requirement R1 Sub Requirement 1.2.5:

CIP-013-1 R1.2.5 is heavily dependent on supplier capabilities and their willingness to provide tools and/or mechanism to enable Registered Entities to perform integrity or authenticity verification. ATC recommends the SDT consider incorporating language that provides flexibility where it is not technically possible.

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	

1. We are concerned about the risks associated with BES Cyber Asset products and services that may contain potentially malicious functionality, are counterfeit, or are otherwise vulnerable due to poor manufacturing and development practices within the industrial control system supply chain. However, the proposed draft standard extends well beyond software authenticity and beyond the ability for entities to manage.

2. New requirements for notification of changes in supplier workforce and incident reporting are impossible to implement and audit due to a lack of a consistent approach and application amongst entities. Industry and industrial supply chain vendors would serve more time sending out notification agreements and attestations than working on making a better and more secure product. Would the supply chain vendor be required to send out a notification every time an employee leaves or finds a virus in the office? If so, then the requirement will be too burdensome for vendors and entities to manage.

3. We believe NERC language in the in the draft standard would have a significant negative impact on the industrial control system community over the long term. As seen in the nuclear industry, specific standards that are outside of other critical sectors will only drive cost up and a willing supply of vendors, down.

4. The need for such a broad set of requirements are unnecessary due to the existing requirement for the entity to have an incident response plan, anti-virus protection and patch management.

5. The additions of *"and, if applicable,* 4 *associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and* 5 *Protected Cyber Assets" in requirement 1 greatly expands the scope of cyber assets.* ACES recommends limiting the cyber assets in scope to BES Cyber Assets.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the Cyber Security Supply Chain Management Technical Conference on November 10, 2016.

As part of Supply Chain Risk Management, Reclamation understands that the risks associated with interaction with vendors, their products, and/or their services are to be considered and mitigated with controls such as contract clauses, physical controls, and/or electronic controls (including vendor remote access). Reclamation recommends that Requirement R1 should instead address the development of one or more supply chain risk management plans that identify risks and controls for mitigating cyber security risks throughout the life cycle(s) of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Within Requirement R1, the life cycle steps to consider in identifying risks and the respective controls should include but not be limited to: evaluation of design, procurement, acquisition, testing, deployment, operation, and maintenance.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Rationale for Requirement R1:

The rationale language for R1 states, “The cyber security risk management plan(s) specified in Requirement R1 apply to BES Cyber Systems." If the intent of the “BES Cyber Systems” reference is to be applicable for all three impact classifications (High, Medium and Low), IPC recommends adding impact classification language.

The rationale language for R1 states, “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.” How does the SDT expect Responsible Entities to demonstrate compliance if existing contracts are acceptable?

The rationale language for R1 states, “The objective of verifying software integrity and authenticity (Part 1.2.5) is to ensure that the software being installed in the applicable cyber system was not modified without the awareness of the software supplier and is not counterfeit.” How does the SDT expect Responsible Entities/vendors to demonstrate compliance with this?

The rationale language for R1 states, “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan." IPC suggests including the verbiage “with vendors, suppliers or other entities executed as of the effective date of CIP-013-1” to the third paragraph of the “Rationale for Requirement R1.”

R1

The requirement language for R1 states, “Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated EACMS, PACS and PCAs.” If the intent of the “BES Cyber Systems” reference is to be applicable for all three impact classifications (High, Medium and Low), IPC recommends adding impact classification language. In addition, if the intent of the “if applicable” reference is to imply “EACMS, PACS and PCAs associated with BES Cyber Systems,” IPC recommends replacing the “if applicable” language with “and their associated” language to remain consistent with current enforceable standard language.

R1.2 – IPC has concerns about the ability of a Responsible Entity to comply with, as written, R1.2, specifically R1.2.1 – R1.2.7. IPC believes there will be instances when vendors (e.g., larger IT vendors, smaller vendors, open source software, etc.) will not agree to provide all of the information necessary to meet the R1.2.1 – R1.2.7 requirements, potentially forcing Responsible Entities to look at other, lower quality options to ensure compliance, or vendors will use the required compliance control(s) as leverage during contract negotiations. The rationale for R1 states, “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan.” However, the rational language does not translate to a release from the R1.2 requirements. How does the SDT foresee Responsible Entities demonstrating compliance when an entity is unable to obtain a specified control(s)? Further, how does the SDT foresee these requirements being measured by auditors?

R1 and R1.2 require the development and implementation of “processes” and/or “plans.” If vendors refuse to agree to terms, what implementation evidence does the SDT expect Responsible Entities to provide? Additionally, if the vendor agrees to the terms stated but fails to deliver according to the documented process, does the SDT foresee this being viewed as non-compliance?

IPC would like to know what additional security measures R1.2.1, R1.2.3, and R1.2.4 provide that aren’t already covered by CIP-007-6, for example CIP-007-6 R2?

IPC recommends adding mitigation plan verbiage to R1.2 requirement language.

M1

The measure language for R1 states, “Evidence shall include (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk management plan(s).” How will this measure apply to Responsible Entities who do not renegotiate or abrogate existing contracts or are unable to obtain specific controls?

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Santee Cooper does not agree with including all BES Cyber Systems in Requirement R1 and suggest using a risk-based approach, to limit this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Santee Cooper believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, Santee Cooper requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Santee Cooper requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

Santee Cooper is concerned about compliance obligations for procurement activities associated with system integrators. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see Santee Cooper’s response to Question #9 for additional information on exceptions).

Santee Cooper notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used. Additionally, Santee Cooper requests that the term be used consistently throughout the standard and not switch between vendor and supplier.

For R1.1.2 requests changing the word *evaluate* to *determine.*

For R1.2.1 Santee Cooper requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. Santee Cooper requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

In Measure M1, Santee Cooper requests that the language be changed to be consistent with the Requirement. Specifically, change “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…” to “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…” (BOLD emphasis added). The construction “address risk” conforms to the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as opposed to mitigated.

Santee Cooper requests that the title of the standard be changed to “Vendor Risk Management” to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term “supply chain risk management” encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although

the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, LCRA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, LCRA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes CIP-013-1 R1 should only apply to High and Medium cyber systems. Applicability to Low systems would potentially place a large burden as current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. BPA requests that the SDT provide clarification as to how R1 would apply to TCAs. 1.2.1 - Is notification under 1.2.1 for what is known at the time of procurement or does it persist after the procurement is fulfilled? What is the time limit? BPA proposes that the language be made consistent with the R1 rationale: “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”	

1.2.2 through 1.2.6 – BPA believes this expands the scope of CIP-004 R5. BPA requests clarification on what this applies to: does it apply to the vendor or to the hardware/software?

The SDT should address gaps that apply to other standards within that standard and not group them into CIP-013-1. For the sub-parts of CIP-013 R1, the scope might be more appropriate in the following locations:

- The topic of access control CIP-013 R1, P1.2.2 is addressed in CIP-004 R5, P5.1
- Vulnerability assessments CIP-013 R1, P1.2.3 is addressed in CIP-010 R3, P3.1
- Cyber security response CIP-013 R1, P1.2.4 is addressed in CIP-008 R1, P1.1
- Software security patches CIP-013 R1, P1.2.5 is addressed in CIP-007 R2, P2.1-2.4; BPA suggests revision to address all patches.
- Interactive Remote Access CIP-013 R1, P1.2.6 is addressed in CIP-005 R2, P2.1.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined in the standard or added to the NERC Glossary of Terms and capitalized when used.

2) For R1: This requirement requires both the development and the implementation of a plan. We recommend modifying this requirement into three steps which follows the CIP-014 structure – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline. The timeline should use fixed dates or intervals and not dates that are linked to the completion of other compliance activities

3) The standard as written addresses Vendor Risk Management and no other supply chain risks such as sole source and international dependencies. Suggest changing the name, purpose, and other areas of the standard from supply chain” to “vendor”.

4) For R1.1.2:

a. We recommend changing *evaluate* to *Determine.* We also seek further clarification of the intent. As, written the requirement is ambiguous:

i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

ii. to evaluate the effectiveness of mitigating that risk? or;

iii. is it meant to identify what controls you have to mitigate the risks you have?

b. The evaluation of methods is a administrative task and similar to other tasks removed from the NERC standards as part of the Paragraph 81 project.

5) For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then this should be an officially defined term either in the standard or in the NERC glossary. The s definition provided in the glossary is “any identified, threatened, attempted or successful breach of vendor’s components, software or systems” and “that have potential adverse impacts to the availability or reliability of BES Cyber Systems” It is unclear if the second portion is meant to be part of the definition. Many cyber systems, like firewalls, are under constant threat and attempts to breach the systems security. Suggest replacing “vendor security event” with “identification of a new security vulnerability”. Vendors may not be able to determine if a vulnerability “could have potential adverse impact to the availability or reliability of BES Cyber System”. This clause would only be applicable in determining when an entity would notify a vendor.

6) For R1.2.1: Page 6, line 12 of the Guidance and Examples document list both notification of security events from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both types of notifications.

7) For R1.2.1: The requirement for the” process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document.

8) Page 6, line 12 of the guidance details the notification of the vendor by the entity. It is unclear that the R1.2.1 requires notification by the entity to the vendor as detail in the guidance document.

9) Recommend that “Security Event” be changed to require the reporting of only newly identified security vulnerabilities.

10) Change 1.2.7 from pointing to 1.1.2 to 1.1.1. Remove 1.2 since 1.2.7 covers 1.2.

11) Do not agree with the current draft language that includes all High, Medium and Low BES Cyber Systems in Requirement R1. Suggests limiting this requirement to High and Medium only as the current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. If controls are needed for low impact, suggest moving these to R5 to consolidate all low impact into a single requirement.

12) The Standard drafting team needs to verify that the SDT needs to make sure that there is no duplication in the standards. Provide guidance on how areas that seem to overlap like Interactive Remote Access and CIP-005.

13) Request the SDT to consider adding the following language from the rationale to the language of the standard “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

14) The Rationale for R1, it states that R1, P1.1 addresses P 56 of Order No. 829. P 56 calls for a risk assessment of the entities internal systems with this language “how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes”. R1, P1.1.1 calls for a risk assessment of the vendors systems with this language “procurement and deployment of vendor products and services.” The language in the order does not match the language in the standard and therefore suggest that the language be consistent to provide clarity.

15) There could be an impact of contract requirements on the ability of public utilities to piggyback on wide-area contracts such as those of National Association of State Procurement Officials (NASPO) Cooperative, Western States Contracting Alliance (WSCA), Washington State Department of Enterprise Service, and others. Recommend that an exclusion be permitted in the case of such contracts, which are important to provide flexibility, effectiveness, and negotiating strength for public utilities throughout the country. In some cases such contracts are required; also include language that provides an exclusion for contracts that are covered by other laws or regulations.

16) The measure should not reference the word mitigation, which to an auditor may limit the actions an entity might take to address risk (such as avoid or transfer). Suggest that “mitigate” be replace with “address” as listed in R1.2.

Likes 1	Austin Energy, 3, Preston W. Dwayne
Dislikes 0	

Response	
Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	
Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	
The FERC order applied to industrial control systems. The SDT is applying the standard to all BES Cyber Assets or systems. It is our belief that all BES Cyber systems are not industrial control systems. The SDT should apply the requirements to industrial control systems such as DCS or EMS systems located in power plants and control rooms.	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Colorado Springs Utilities (CSU) has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.	

CSU does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CSU requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CSU believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CSU requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CSU requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CSU is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see CS's Uresponse to Question #9 for additional information on exceptions).

CSU notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CSU requests changing the word *evaluate* to *determine.*

For R1.2.1 CSU requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CSU requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CSU requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

In Measure M1, CSU requests that the language be changed to be consistent with the Requirement. Specifically, change “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…” to “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…” (BOLD emphasis added). The construction “address risk” conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as opposed to mitigated.

CSU requests that the title of the standard be changed to “Vendor Risk Management” to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term “supply chain risk management” encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013

address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The Rationale for R1 states, “Implementation of elements contained in the entity’s plan related to Party 1.2 is accomplished through the entities procurement and negotiation process.” The SDT need to define the process for determining the minimum level deemed to be sufficient. Additionally, the SDT needs to identify the course of action an entity must take and document where a vendor is unwilling or unable to meet the obligations set forth for Responsible Entities.

R1. In FERC Order No. 829, paragraph 59 states, “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.” The Order does not address requirements for EACMS, PACS, or PCA as identified in R1. The SDT should limit the requirement to the context of the Order.

R1.1.1. The obligation to “identify and assess risks” is extremely open-ended and ambiguous. In contrast, the draft Technical Guidance and Examples document enumerates a list of 11 factors that should be considered in an entity’s plan. NERC standards should be clear on their face, and it is inappropriate to require and entity to refer to draft Technical Guidance and Examples document for fundamental questions concerning whether an entity is compliant with a given requirement. If the Drafting Team believes that this list of 11 factors within the draft Technical Guidance and Examples document is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, an alternate list of factors should be provided. Without clear requirements on the factors to be considered, there is substantial risk in inconsistency of implementation by entities.

R1.1.1. The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production. To avoid confusion, the term “deployment” should be removed.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx

Comment

The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.

Seattle City Light has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Seattle City Light does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, Seattle City Light requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Seattle City Light believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, Seattle City Light requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Seattle City Light requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

Seattle City Light is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. In some cases use of these contracts in procurement is mandated by other laws or regulations. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see Seattle City Light’s response to Question #9 for additional information on exceptions).

Seattle City Light notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 Seattle City Light requests changing the word *evaluate* to *determine.*

For R1.2.1 Seattle City Light requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 Seattle City Light requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. Seattle City Light requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

In Measure M1, Seattle City Light requests that the language be changed to be consistent with the Requirement. Specifically, change “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…” to “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…”

(BOLD emphasis added). The construction "address risk" conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as alternatives to being mitigated.

Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.

Likes 0	
Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3

Answer	No
Document Name	

Comment

FEUS supports the comments submitted by APPA

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response

Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	

It is unclear how the risk and requirements in R5 for Low Impact BES Cyber Systems are differentiated from the other requirements and how the requirements will be measured considering a list of Low Impact systems are not required. There seems to be some reduncancy between R1 and R5 for Low Impact. Suggest removing Low Impact requirements from CIP-013 and incorporating into CIP-003 for consitency.

Likes 0	
Dislikes 0	
Response	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	

Ambiguity in R1

FERC Order No. 829 asks for a plan to be developed and implemented by the entity that **includes** security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. It recognizes the diversity of BES Cyber System environments, technologies and risks among entities. FERC states that the “Reliability Standard may allow a responsible entity to meet the security objectives discussed below by having a plan to apply different controls based on the criticality of different assets.”

We find that the use of word “address” in R1 is creating ambiguity.

We suggest that requirement should be clear in stating that entities are to identify supply chain cyber security risks, evaluate controls and select controls, and implement controls based on their acceptable risk levels for future procurement contracts.

In doing so, entities should consider, at minimum, the controls that are itemized in the FERC Order and evaluate whether implementation of those controls are appropriate based on risk.

The four objectives that R1 should address are not clear

FERC Order states the “following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., 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”)).”

The required plan is not tied to the objectives stated in the FERC Order.

1. For Information System Planning, FERC Order appears to ask that the responsible entity must include security considerations as part of its information system planning and system development lifecycle. The information system planning and development lifecycle should be periodically reviewed and approved by CIP Senior Manager.

We believe that R1.1 is intended to address the Information System Planning objective in the FERC Order. Consideration of security risks in Information System Planning is the objective of the overall plan.

R1.1 causes ambiguity. It is not clear how controls can be used to identify and assess risk. Controls are used to mitigate risk. Evaluation of controls is performed prior to their selection depending on the acceptable level of risk and cost associated with the controls. The verbiage of Part 1.1.2 requires controls for the evaluation of methods to address risks. It does not require risks to actually be determined.

2. R1.2 lists a number of controls (some specifically stated in the FERC Order) and does not identify which objective these controls are to address.

a. For Software Integrity and Authenticity objective, FERC Order appears to ask that at minimum, entities should consider implementing the following controls to mitigate risk by:

1. Verifying the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and

2. Verifying the integrity of the software and patches before they are installed in the BES Cyber System environment. (R1.2.5)

The Standard appears to address this objective in Requirement 3. There is overlap/redundancy between R1.2.5 and Requirement 3.

b. For Vendor Remote Access to BES Cyber Systems, FERC Order appears to ask that at minimum, entities should consider implementing controls to mitigate risk by Logging and controlling all third-party (i.e., vendor) initiated remote access sessions including user-initiated and machine-to-machine vendor remote access. (R1.2.6)

The Standard appears to address this objective in Requirement 4. There is overlap/ redundancy between R1.2.6 and Requirement 4.

c. For Vendor Risk Management and Procurement Controls, FERC Order appears to ask that at minimum, entities' controls should consider implementing controls to mitigate by means of:

1. Vendor security event notification processes; (R1.2.1)

2. Vendor personnel termination notification for employees with access to remote and onsite systems; (R1.2.2)

3. Product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (R1.2.3)

4. Coordinated incident response activities; and (R1.2.4)

5. Other related aspects of procurement. (R1.2.7)

Related to R1.2.1, It is not clear what constitutes a "vendor security event". Every vendor may have a different consideration for what constitutes a "security event". It could include an instance of employee fraud, workplace assault, or even the announcement of a patch release.

Related to R1.2.4, Cyber Security Incident is a NERC defined term. Is a cyber security incident a Cyber Security Incident? If not, what is the distinction? If it is, the term will need to be capitalized. Also the term "vendor related cyber security incident" is not clear. Is it a Cyber Security Incident that could happen during procurement and deployment stage?

We also find R1.2.7 is unnecessary and creates ambiguity.

Applicability

FERC Order suggests that entities can perform their own assessment of risks and determine applicability of controls based on that.

It is not clear how the described controls are applicable to BES Cyber Systems based on their risk level in the context of CIP Standards (Low, Medium, and High).

The Standard extends applicability to the EACMS, PACS, and PCAs associated to BES Cyber Systems. We argue that PACS, EACMS and PCAs, although are important for Physical and Electronic Security, are not necessarily “industrial control system hardware, software, and computing and networking services associated with bulk electric system operations” as stated in the FERC Order.

This standard should not be applied to systems or assets not needed for BES operations.

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

Sacramento Municipal Utility District (SMUD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

SMUD does not agree with including all BES Cyber Systems in Requirement R1. SMUD supports a risk-based approach, while limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, SMUD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, SMUD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

SMUD requests that the SDT add the following language from the rationale to the language of the standard: "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

SMUD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see SMUD's response to Question #9 for additional information on exceptions).

SMUD notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 SMUD requests changing the word *evaluate* to *determine.*

For R1.2.1 SMUD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 SMUD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. SMUD requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Requirement Placement (CIP-013 versus CIP-003)

R1 (and R2) includes low, medium, and high BES Cyber Systems; however, the current CIP Standards put the low impact BES Cyber Systems (LIBCS) requirements in CIP-003. EEI recommends that the SDT consider whether to move the LIBCS requirements from CIP-013 into CIP-003. Moving the LIBCS to CIP-003 may make it easier for Responsible Entities with only LIBCS to implement the requirements.

However, Responsible Entities with high, medium, and low impact BES Cyber Systems (HIBCS, MIBCS, and LIBCS) may be concerned that moving the supply chain LIBCS requirements to CIP-003 may make it difficult for them to take a holistic approach to the CIP-013 requirements. For example, some entities may want to focus on their BES Cyber System vendors and apply a single vendor-based approach for HIBCS, MIBCS, and LIBCS. Also, CIP-013 is focused on the risk that vendors and suppliers may introduce into BES Cyber Systems, whereas the other CIP Standards are focused on more general cybersecurity risks that can be addressed by Responsible Entity operational controls, which are within the control of the Responsible Entity. Third-party risk is harder for Responsible Entities to control and the methods of control are more likely contractual than operational. For example, a Responsible Entity cannot control a vendor's manufacturing process, but can ask questions during procurement as to how security risk is managed by the vendor to help evaluate the level of risk the vendor may pose to the Responsible Entity. As a result, there may be value in keeping these requirements out of the other CIP Standards, which focus on operational controls for cybersecurity risk.

Applicable Systems

Requirement R1 applies to LIBCS as well as HIBCS and MIBCS and their associated EACMS, PACS, and PCAs. We do not believe that EACMS, PACS, and PCAs should be included under the scope of Requirement R1. The diversity and sheer number of these systems make it difficult to document how Responsible Entities will address procurement for all of these systems in their risk management plans. Auditing these plans will also be difficult.

Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor's product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement's objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using "industrial control systems associated with BES Cyber Systems" may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.

Security Objective

The security objective of Requirement R1 is unclear. Although it focuses on the Commission objectives 3 and 4, it would be helpful to make it clear in the requirement language so that Responsible Entities understand the purpose of the requirement.

Objective 3 is focused on making sure that Responsible Entities do not unintentionally plan to procure or fail to anticipate security issues during procurement or technology/vendor transitions. Objective 4 is focused on ensuring security concepts are addressed in future contracts. Both of these objectives are focused on evaluation of the risk that the vendor or vendor product/service may introduce to the BCS by the Responsible Entity during planning for and actual procurement of new systems. The controls that are required under Requirement R1 are also not operational controls, but process controls to assess and evaluate the risk.

Risk Acceptance

We understand that Order No. 706 ordered the ERO to remove acceptance of risk language from the CIP Reliability Standards. In this case, it was tied to a concern over uncontrolled compliance exceptions to addressing potential vulnerabilities and the Commission preferred the use of technical feasibility, which led to technical feasibility exceptions. (See Order No. 706, P 150-151) We are not recommending the use of "acceptance of risk" in CIP-013, but we want to make it clear that risk acceptance may be a good option in dealing with procurement controls (CIP-013, Requirement R1), which are different than the operational controls covered by the other CIP Standards.

The security objective for Requirement 1 is focused on Responsible Entity awareness of risk that may be introduced by the vendor or vendor product/service. The Responsible Entity's ability to control this risk is limited. For example, the Responsible Entity may only have a few vendors to choose from for a particular procurement and the vendors may not have a well-defined process for vendor security event notification. The Responsible Entity can ask them to define a process and can even put language into a contract to require such a contract, but the vendors can say no. The Responsible Entity is left with the choice of either not procuring this device or system or accepting the risk. Documenting a compliance exception for every term the vendor does not agree to does not seem reasonable in light of the scope of Requirement R1 – the sheer numbers of systems covered (HIBCS, MIBCS, and LIBCS) and diversity of vendors for each of these systems and system components. Responsible Entities also cannot make the vendor develop or follow this process even if the vendor agrees to, which is also a consideration for the SDT – if the vendor does not comply with their contract terms is the Responsible Entity subject to a violation and penalty?

We recommend that the SDT consider, set, and articulate compliance expectations with Requirements R1 and R2 and recognize the difference between these procurement controls and the operational controls found in the rest of the CIP Standards.

Measure M1

We are concerned with the M1 language use of "written agreements" as a measure of plan implementation, even though it is introduced with "could include, but is not limited to." Requirement R1 does not (and should not) require Responsible Entities to use contract terms to meet the security objective. However, contract terms may be one method of "how" to meet the security objective ("what"), but not all entities will choose this "how". We are concerned that the inclusion of "written agreements" in the measure text suggests that this is a key piece of evidence for compliance with R1. Also, the use of "correspondence" in M1 could include "written agreements" if an entity chooses to use them for R1. We recommend removing "written agreements in electronic or hard copy format" from M1.

We recommend the following language for consideration by the SDT:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) to minimize the cyber security risks from vendors and vendor products and services to BES Cyber Systems during planning and procurement of industrial control systems. The plan(s) should address one or more methods to:

1.1. Raise awareness of risk the vendor and vendor product or service may introduce, including awareness of vendor process(es) to:

1.1.1. Notify the Responsible Entity of vendor security events;

1.1.2. Notify the Responsible Entity of when vendor employee remote or onsite access should no longer be granted;

1.1.3. Disclose known vulnerabilities to the Responsible Entity;

1.1.4. Coordinate the response to vendor-related cyber security incidents with the Responsible Entity;

1.1.5. Verify the software integrity and authenticity of vendor software and patches; and

1.1.6. Control remote access, including vendor-initiated interactive remote access and system-to-system remote access to the Responsible Entity

1.2. Assess risk(s) introduced by the vendor and vendor product or service identified by Part 1.1; and

1.3. Evaluate method(s) to address risk(s) identified by Part 1.2.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language. Particularly R1 should only focus on supply chain risk management during the procurement phase rather than controls during operations. Operational controls on BES systems should be covered in other CIP standards. Furthermore, if controls are to be required on a vendor's manufacturing process, in addition to those identified during RFP negotiations, these controls should be consistent and verifiable by an industry standard (similar to ISO(?) 9001 certification).	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, LCRA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, LCRA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.	
Likes 0	
Dislikes 0	
Response	

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Many of the aspects of CIP-013-1 R1 cannot be controlled by the entity, but instead need to have assurances from the vendor. In other CIP standards there are operational controls that the entity can make to meet the requirements of the standards; these controls are things the entity can control.

The scope of R1 includes BCAs, EACMS PACS and PCAs with no guidance concerning the risk associated with each of these types of assets. Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor's product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement's objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using "industrial control systems associated with BES Cyber Systems" may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.

Likes 0	
Dislikes 0	
Response	

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	

The IRC and SWG thanks the Drafting Team for their work and support the concepts in the security program enhancements addressing supply chain risks.

The Rationale for R1 states, "Implementation of elements contained in the entity's plan related to Party 1.2 is accomplished through the entities procurement and negotiation process." The SDT need to define the process for determining the minimum level deemed to be sufficient. Additionally, the SDT needs to identify the course of action an entity must take and document where a vendor is unwilling or unable to meet the obligations set forth for Responsible Entities.

R1. In FERC Order No. 829, paragraph 59 states, “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.” The Order does not address requirements for EACMS, PACS, or PCA as identified in R1. The SDT should limit the requirement to the context of the Order.

R1.1.1. The obligation to “identify and assess risks” is extremely open-ended and ambiguous. In contrast, the draft Technical Guidance and Examples document enumerates a list of 11 factors that should be considered in an entity’s plan. NERC standards should be clear on their face, and it is inappropriate to require and entity to refer to draft Technical Guidance and Examples document for fundamental questions concerning whether an entity is compliant with a given requirement. If the Drafting Team believes that this list of 11 factors within the draft Technical Guidance and Examples document is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, an alternate list of factors should be provided. Without clear requirements on the factors to be considered, there is substantial risk in inconsistency of implementation by entities.

R1.1.1. The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production. To avoid confusion, the term “deployment” should be removed.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Many of the aspects of CIP-013-1 R1 cannot be controlled by the entity, but instead need to have assurances from the vendor. In other CIP standards there are operational controls that the entity can make to meet the requirements of the standards; these controls are things the entity can control.

The scope of R1 includes BCAs, EACMS PACS and PCAs with no guidance concerning the risk associated with each of these types of assets. Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor’s product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement’s objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using “industrial control systems associated with BES Cyber Systems” may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

Q1-Issue1-Discussion

(1) In reviewing the measures M1, R1 is written in a manner to collect evidence to achieve two objectives; (i) documentation of the plan, and (ii) documentation to demonstrate implementation of the plan(s). According to NERC's Drafting Team Reference Manual which was recently revised and published October 19, 2016, on page 11 under section B – Requirements and Measures (http://www.nerc.com/pa/Stand/Resources/Documents/Drafting%20Team%20Reference%20Manual_Oct2016_final.pdf), each requirement should "achieve one objective." The Reference Manual goes on to state: *If a requirement achieves two objectives, such as developing a document and distributing that document, then each objective should be addressed in its own requirement.* Contrary to instructions delineated in the Reference Manual, R1 requires Entities meet two objectives, develop **and** implement the supply chain risk management plan.

Q1-Issue1-Recommendation

GTC recommends R1 be separated into two separate requirements where the first objective of the FERC directive identified in paragraph 2 is addressed to "develop a plan" (R1), and the second objective is addressed in its own requirement to "implement the plan" (new R2). This method simplifies compliance documentation for the Responsible Entity and aligns with the principles documented in NERC's Reference Manual. Additionally, this method will simplify and provide clarity to achieve FERCs directive for the plan to be forward-looking as explained in further detail below.

Q1-Issue2-DISCUSSION

(2) The SDT has clarified in the rationale for requirement R1 that the implementation of the cyber security risk management plans(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 as specified in the Implementation Plan. Additionally, Paragraph 59 stipulates to address security concepts in "future contracts". However, GTC does not see this forward looking language in the actual Requirement R1 that is specified by the FERC Order. GTC believes this forward looking language can be better clarified and highlighted if the SDT accepts GTC's first recommendation to separate R1 into two requirements and "implement the plan" is written as its own requirement.

Q1-Issue2-Recommendation

GTC recommends the following:

Separate R# to implement plan(s), then update the new Requirement with the following language: "Each Responsible Entity shall implement the documented supply chain risk management plan(s) specified in Requirement R1. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

Q1-Issue3-DISCUSSION

(3) Paragraph 45 of Order No. 829, clearly specifies “The Plan” should address, at a minimum, four specific security objectives in the context of addressing supply chain management risks.

(P. 45) The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Although R1 technically covers the four specific security objectives, the presentation lends itself somewhat confusing. R1.2.5 seems to align with security objective (1), R1.2.6 seems to align with security objective (2), and are both subsets to R1.2 which seems to align with security objective (4).

Q1-Issue3-Recommendation

GTC believes R1 will be clearer to understand and that the drafting team could gain more support if the four specific security objectives required by Order 829 Paragraph 45 had their own individual sub-requirement of “The Plan”, in lieu of sub-requirements of one of the security objectives such as:

R1.1 aligns with security objective 3 (*information system planning*) where the specifics of the third objective identified in paragraph 56 is captured as a subset of R1.1;

R1.2 aligns with security objective 4 (*vendor risk management and procurement controls*) where the specifics of the fourth objective identified in paragraph 59 is captured as a subset of R1.2;

R1.3 to align with security objective 1 (*software integrity and authenticity*) where the specifics of the first objective identified in paragraph 48 is captured as a subset of R1.3; and

R1.4 to align with security objective 2 (*vendor remote access*) where the specifics of the second objective identified in paragraph 51 is captured as a subset of R1.4.

Q1-Issue4-DISCUSSION

(4) Order 829 Paragraph 58 refers to NIST Special Publication 800-53 for various supply chain development life cycle controls. The definition of Supply Chain from NIST SP 800-53 r4 states that the “supply chain horizon" ends at the delivery of products/services to the acquirer. FERC Order 829 acknowledges this definition in paragraph 32, footnote 61.

Supply Chain: “Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer”

Accordingly, in the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur “upon commissioning” for planned system installations (and even later for unplanned changes). Therefore, BES Cyber System identification, categorization as high, medium, or low impact; and also identifying associated EACMS, PACS, and PCAs does not exist during the supply chain context. Therefore, R1 should be limited to a supply chain risk management plan which will address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services of Cyber Assets which are intended to support Bulk Electric System operations as specified in Order 829 paragraph 43.

Q1-Issue4-Recommendation

GTC recommends the SDT adopt the aforementioned NIST SP 800-53 defined term Supply Chain for use with CIP-013-1 R1 in front of the term “risks” to contain the Time Horizon to supply chain risk management, and also edit to account for the fact that BES Cyber System identification and categorizations do not exist during the supply chain context.

An example of R1 is provided:

R1. Each Responsible Entity shall document a Supply Chain risk management plan(s) that address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services which are intended to support Bulk Electric System operations. The plan(s) shall address:

R1.1 The use of controls for mitigating Supply Chain risks associated with *information system planning*

R1.2 The use of controls for mitigating Supply Chain risks associated with *vendor risk management and procurement controls*

R1.3 The use of controls for mitigating Supply Chain risks associated with *software integrity and authenticity*

R1.4 The use of controls for mitigating Supply Chain risks associated with *vendor remote access*

Q1-Issue5-DISCUSSION

GTC disagrees with the inclusion of associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets in requirement R1. GTC finds no reference to the inclusion of these associated systems in FERC Order 829 and recommends their removal from this standard.

Further, GTC questions whether the use of the term BES Cyber Systems is appropriate in a standard which is limited per FERC Order 829 to “the context of addressing supply chain management risks.” In the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur “upon commissioning” for planned system installations (and even later for unplanned changes). Therefore, BES Cyber System identification, categorization as high, medium, or low impact; and also identifying associated EACMS, PACS, and PCAs does not exist during the supply chain context.

Q1-Issue5-Recommendation

GTC recommends the removal of any reference to Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. GTC recommends removal of references to BES Cyber Systems and replacing it with the phrase “hardware, software, and computing and networking services which are intended to support Bulk Electric System operations.”

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

R1.1 is acceptable in regard to requiring entities to have a plan to identify and assess risks with procured equipment. R1.2 is unacceptable because Entity creation of Detective Controls for the four Objectives of P. 45 is considered out of the Entity's scope. If only one Entity and one Vendor existed, the individual sub-parts of R1.2 may be feasible for control planning – but this approach is not viable for hundreds of entities and dozens of vendors. The Entity is capable of identifying Preventative Controls, in concept, but they will only be effective if all the vendors in the supply chain make a diligent effort to implement the controls all the way back to the first-line suppliers. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich

Answer	No
Document Name	

Comment

See comments submitted by Black Hills Corporation

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
The requirement should focus on the risk of the software or services being procured and not allow for the possibility of a Registered Entity taking a risk view based upon the impact categorization of the BES Cyber System or EACMS, PACS, or PCA that is affected by the procurement. The requirement needs to clearly be focused on the vendor processes without regard to the Cyber Assets impacted by the vendor. The controls need to include processes for granting vendor access in addition to the processes for notifying when removal of access is necessary. The controls to grant access should include expectations for the conduct of training and personnel risk assessments, including review, modification as necessary, and acceptance of the vendor's process by the Registered Entity, if applicable, along with expectations of what evidence of compliance will be provided to the Registered Entity by the vendor. Part 1.2.4 should include an expectation of notification by the vendor in addition to coordination of the response.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	
1) The Rational for Requirement R1 includes a definition of the term "vendors". This definition is also included in the Guidelines and Examples document. This term should be officially defined.	

2) It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3) R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

For R1: With respect to the obligation to “identify and assess risks,” the standard is extremely open-ended. In contrast, the Compliance Guidance enumerates a list of 11 factors that should be considered. NERC standards should be clear on their face, and it should not be necessary to refer to Compliance Guidance for basic questions concerning whether an entity is in compliance with a given requirement. If the Drafting Team believes that this list of 11 factors is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, a complete list of factors should be provided. Without clear guidance, as to factors that should be considered, there is substantial compliance risk if a subjective auditor disagrees with the risk factors identified by an entity

R 1.1.1 – The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production (i.e. once deployed). To avoid confusion, the term “deployment” should be removed or clarified.

4) For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5) For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6) For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list “planning, acquisition and deployment” and versions of these terms in the diagram. R1.1 uses “planning and development”. The meaning of “development” has not been clarified and is not part of the process addressed by this standard. Suggest that “development” be clarified or removed.

7) For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

b. To evaluate the effectiveness of mitigating that risk? or;

c. Is it meant to identify the controls in place to mitigate the identified risks?

8) For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then” Security Event” should be replaced or clarified in the Requirement. This clarification could include “any identified, threatened, attempted or successful breach of the vendor’s components, software or systems used in the support of the Entity’s BES Cyber System.” This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3

9) For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

10) For R1.2.2: The requirement for the” process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document the requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that “A failure of a vendor to follow a defined process is not a violation of this Requirement.”

For R1.2: A newly added (in the 1/19/17 draft) sentence in the Rationale (R1) section states: “Implementation of elements contained in the entity’s plan related to Part 1.2 *is accomplished* through the entities procurement and negotiation process. Who determines whether it was a sufficient effort to “implement the elements” as part of the procurement and negotiation process? What if you take their first “no” for an answer – is that sufficient effort to implement? Who gets the final sign off?

11) Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an *existing contract*? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard.

Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1

The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

“Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

“Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	

Comment

- What is meant by “if applicable” in the Requirement. If this means EACMS/PACS/PCAs for high and medium impact BES Cyber Systems, then state this.
- Extending the applicability to all BES Cyber Systems and associated EACMS/PACS/PCAs results in an unfathomable expansion in scope. For example, in a small Medium Impact Control Center BES Cyber System, we have between 50 and 60 individual software and hardware contracts to manage. Most common industry practices would base the procurement policies for these contracts based on their financial risk, or contracts above a certain spending threshold. However, managing cyber risk does not relate to spending. A million-dollar EMS system could carry less cyber security risk than a $20 camera or a one thousand-dollar network switch. This implies a centralized procurement office for all purchases, since each potential purchase needs to be evaluated for the Cyber Security risk it presents. This would have tremendous costs for smaller entities. We suggest limiting the scope to high and medium impact BES Cyber Systems.
- 1.2.3 should read “known [security] vulnerabilities”. Vulnerabilities include any weakness in the code.
- What does coordination mean in 1.2.4 and 1.2.6?
- Remove 1.2.7. This does not belong in a mandatory and enforceable Standard. As it stands, an entity is required to add other indeterminate processes.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
R1.1 is acceptable in regard to entities having a plan to identify and assess risks with procured equipment. R1.2 is unacceptable because the entity creation of Detective Controls for the four Objectives of P. 45 is considered out of the Entity's scope. If only one Entity and one Vendor existed, the individual sub-parts of R1.2 would be feasible for a control plan – but this approach is not viable for hundreds of Entities and dozens of vendors. The Entity is capable of identifying Preventative Controls, in concept, but they will only be effective if the vendors in the supply chain make a diligent effort to implement the controls to the first-line suppliers. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified.	
Likes 0	
Dislikes 0	
Response	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
FERC didn't specifically ask for Low Impact BES Cyber Systems to be included but didn't explicitly exclude them either. SunPower does not believe Low Impact Cyber Systems should have to meet the same expectations of High and Medium Impact Cyber Systems. While we appreciate the efforts of the SDT to meet the expectations of the FERC Order, we believe the SDT may have gone beyond what FERC was asking them to do. CIP-003-6 does not require Entities with Low Impact Cyber Systems to have to list the BES Cyber Systems, with this new requirement, do Entities lose their exception? If there is an expectation of that Low Impact Cyber System Entities must adhere to the same or lesser requirements as High and	

Medium Impact Cyber System Entities, then perhaps CIP-003 would be a better place for the exception. SunPower believes CIP-013, as written, is in direct conflict with the intent of CIP-003-6.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 1. In addition, we offer the following comments: **Remove Identify, Assess, and Control Found at the Requirement Level** We suggest deletion of these words and terms. The use of identify, assess, and control (IAC) is represented by the responsible entity's governance and control structure. This is an evaluation performed by the Regional Entity in evaluation of the responsible entity's inherent risk and oversight model.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
Oxy disagrees that R1 should be applicable to low impact BES Cyber Systems. Although FERC is silent on whether low impact should be included, Paragraph 2 of Order No. 829 says "nor does the Commission require NERC to propose "one-size-fits-all" requirements. The new or modified Reliability Standard 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." The language of R1 elevates low impact BES Cyber Systems to the level of medium and high impact BES Cyber Systems. For example, R 1.2.2 requires a process for when vendor employee remote or onsite access should no longer be granted. Under existing CIP Standards, Access Management Program requirements reside in CIP-004 and none are applicable to low impact BES Cyber Systems. R 1.2.5 requires processes for verifying software integrity and authenticity of all software and patches that are intended for use. Under existing CIP Standards, Security Patch Management requirements reside in CIP-007 and none are applicable to low impact BES Cyber Systems. Additionally, software and patching typically occurs at the Cyber Asset level and low impact entities are only required to identify assets containing low impact BES Cyber Systems. As currently written, R1 and its sub-requirements seem to require an inventory of Cyber Assets or BES Cyber Systems, neither of which are required of low impact entities, which is another element that elevates low's to	

that of medium and high. Using a risk based approach, it seems more appropriate that R1 be applicable to medium impact and high impact only. The risk assessments are required and performed under CIP-002 and the determination made that low impact BES Cyber Systems pose a minimal threat to the BES. Finally, under the existing CIP suite of standards, requirements applicable to low impact entities reside in CIP-003. If a risk management plan is to be required, low impact with a reduced set of requirements to address their minimal BES risk, Oxy requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5. Oxy also requests that CIP-013-1, R1 be rewritten to be applicable to medium and high impact BES Cyber Systems only.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

- Regarding R1.2.1, vendors will unlikely to share security events. Registered Entities should not be held accountable for compliance obligations in which they have no control of.
- Regarding R1.2.1, the Standard Drafting Team should clarify what is intended by, “vendor security event.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.3, the Standard Drafting Team should clarify what is intended by, “known vulnerabilities.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.4, the Standard Drafting Team should clarify what is intended by, “cyber security incidents.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.4, vendors will be unlikely to share cyber security incidents. Registered Entities should not be held accountable for compliance obligations in which they have no control of.
- Regarding R1.2.5, this requirement is duplicative of CIP-007-6. The Standard Drafting Team should clarify how proposed requirement would be completed within the Procurement phase.
- Regarding R1.2.6, this Requirement is duplicative of CIP-005-5.

.

Likes 0	
Dislikes 0	

Response

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No

Document Name	
Comment	

The scope of the requirement is not clear due to the phrase "if applicable." Please clarify how an entity would determine if their Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets are applicable.

Due to some vendors offering many of their products and services outside of the electric utility industry (Microsoft, Cisco, Symantec, GE…) there is a concern that entities will lack leverage when negotiating these new terms and will likely find it difficult to come to an agreement. There are also instances where there are very few options available to industry for a particular product, device, or service. Does the SDT envision that registered entities would be forced to find alternative vendors or products if they are unable to come to an agreement?

It is not clear if the requirements are only applicable to new software purchases or also apply to upgrades of existing software (including adding additional licenses for existing software) or renewals of software maintenance contracts that provide software upgrades of existing software. If the existing software is already in place, there is concern that there will be the lack of leverage to require vendors of existing software to negotiate new terms.

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	

Concur with EEI’s Position

Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	

SVP agrees with other entity comments to limit this requirement to High and Medium only, as current low impact requirements does not require entities to conduct an inventory of equipment and software or identify systems. Pleas also see APPA's comments, with which SVP is in agreement.

Likes 0	

Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	

Comment
The need for such a broad set of requirements is unnecessary due to the existing CIP requirements for the entity to have an incident response plan, anti-virus protection and patch management. To the extent the following items remain in R1, NRECA proposes the following actions: R1.2 – Recommend deleting text after “BES Cyber Systems” as the text is unnecessary. R1.1.1 – Clarify what is meant by “vendor security events.” R1.2.3 – What is the basis for determining what are “known vulnerabilities?” R1.2.4 – Clarify the scope of this language as it seems unnecessarily open-ended. R1.2.5 – Clarify that this item is for BES Cyber Systems only. R1.2.7 – Delete as it is unclear and unnecessarily open-ended.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	

Comment
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns: The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that “address process(es),” and yet, the contents of the requirements include “verifying software integrity.” Responsible Entities are familiar with various existing CIP requirements that mandate the development of “processes,” but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take

and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns:

The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that "address process(es)," and yet, the contents of the requirements include "verifying software integrity." Responsible Entities are familiar with various existing CIP requirements that mandate the development of "processes," but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	

The applicability of this requirement should be limited to high and medium impact BES Cyber Systems. Low impact Cyber Systems are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES. We can re-evaluate at a later date whether additional requirements should be established for low impact BES Cyber Systems.

Using “if applicable” adds confusion to the language. If it is not always applicable to associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets, define where it is applicable and where it is not.

We’re concerned that the word “Evaluate” in requirement 1.1.2 might imply that all possible methods for addressing the risks will need to be evaluated. We prefer replacing the term “Evaluate” with “Identify”. Additionally, there may be occasion where a risk is identified but is judged to be at an acceptable level given the ability or inability to address it. This standard, in its entirety, should be about minimizing the risks and/or providing reasonable assurance which may result in some instances where the entity will accept a certain level of risk as reasonable. Therefore, we propose the following language: 1.1.2. Identify methods to address the above risk(s), as needed.

Requirement 1.2.1 requires “Process(es) for notification of vendor security events”. CIP-007-6 R4 Security Event Monitoring includes a requirement for generating alerts for security events. Assuming that Requirement R1.2.1. is intended to mean the entity will have a process to encourage and direct vendor notification to the client, we suggest this be included in the language of CIP-007.

Requirement 1.2.2 requires “Process(es) for notification when vendor employee remote or onsite access should no longer be granted” The revocation of access, including Interactive Remote Access is currently addressed in CIP-004-6 R5. If this is attempting to require something above and beyond those requirements, it should be made clear what that is and consideration given to housing all of these requirements in CIP-004.

Requirement 1.2.3 requires “Process(es) for disclosure of known vulnerabilities”. Is this asking for entities to have a process for the entity to disclose vulnerabilities? Who would we be disclosing to? If it’s directed at vendors, the entity can discuss this with the vendor, but the vendor is under no obligation to disclose vulnerabilities and neither the entity, nor FERC, has the authority to require this. Vendors MAY disclose vulnerabilities, but that will likely occur concurrent with providing a fix/patch.

Requirement 1.2.4 requires a “Coordination of response to vendor-related cyber security incidents”. From our understanding of what this requires, we believe this is already covered in the entities cyber security incident response plan (CIP-008).

Requirement 1.2.7 requires “Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable”. While we understand what this requirement is intending to do, we believe it is may lead to second-guessing by auditors and/or unrealistic auditor expectations.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns:

The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that "address process(es)," and yet, the contents of the requirements include "verifying software integrity." Responsible Entities are familiar with various existing CIP requirements that mandate the development of "processes," but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	Final_Unofficial_Comment_Form_2016-03_03162017_ERCOT comments.docx

Comment

ERCOT supports the IRC comments and offers the following supplemental comments.

FERC Order 829, Paragraph 59, states that NERC's new or modified 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." This does not include the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) listed in R1. These systems do not perform or provide bulk electric system operations. ERCOT believes the inclusion of these systems in the draft standard goes beyond the scope of the standard intended by FERC and recommends the SDT remove them from the applicable systems of the standard language.

Requirement R1 requires Responsible Entities to have a plan that addresses processes for notification of a vendor's cyber security events (R1.2.1) and vulnerabilities (R1.2.3), as well as coordination of cyber security incident response activities (R1.2.4). As this information is highly sensitive, it is unlikely that all vendors will agree in all cases to provide this information unless they are already required to do so under other regulatory obligations. Responsible Entities cannot force a vendor to agree to these terms, and in cases where the vendor deems the risk of this disclosure too great compared to the value of the contract, the vendor will decline to enter into the agreement. This will force the Responsible Entity to seek another vendor that is

willing to accept these terms, and such a vendor may or may not exist. Because it is possible that a Responsible Entity may be unable to identify a vendor that is willing to accept a contract with the terms required by R1, the proposed standard could seriously hamper the essential functions of Responsible Entities. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R1. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Requirement R1.2.2 requires "notification when vendor employee remote or onsite access should no longer be granted." The revocation of access, including Interactive Remote Access, is currently addressed in CIP-004, R5. Since the background checks, training, access authorization, and access revocation for employees and vendors is already addressed in CIP-004, the drafting team should ensure any new requirements related to access revocation of vendors be placed in CIP-004. In developing the CIP Version 5 standards, extensive work was undertaken to ensure that all requirements related to the subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework.

Requirement R1.2.5, which requires a Responsible Entity's plan to include "Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use," is duplicative of Requirements R3 and R5 within this standard, which also require documentation of processes. ERCOT recommends removing R1.2.5.

Requirement R1.2.6 requires an entity's plan to include "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)." This requirement is duplicative of Requirement 4 within this standard. ERCOT recommends removing Requirement R1.2.6, which also requires documentation of processes.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes

Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Requirement R1 states “supply chain risk management plan(s)” while M1, R2, M2 states “supply chain cyber security risk management plan(s)”. ReliabilityFirst recommends the SDT use consistent language so that there is no confusion on terminology.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
While in overall agreement with Requirement 1, ACEC does have the following concerns: 1. Part 1.1 requires the Responsible Entity to identify and assess risk(s) and evaluate methods to address identified risks. This requirement specifically changes the methodology for risk assessment defined in CIP-002-5.1. As noted in the Background section (Section 6) of the standard, "This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards." This view of risk based upon the impact of BES Cyber Assets based upon the impact to the BES, not the devices cyber security risk, was defended by NERC and approved by FERC in Order 791 approving Version 5 of the CIP Standards. Based upon this, it would be consistent with CIP-002-5.1 to remove Part 1.1 of Requirement 1, modify requirement R1, Part 1.2.7 to state "other process(es) to address risk(s) as determined in CIP-002-5.1 R1, Parts 1.1 and 1.2" and to add to requirement R1 that it only applies to high and medium impact BES Cyber Systems as used in R3 and R4. 2. In the Rationale for Requirement R1, the term vendor is defined as "(i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators." ACEC is concerned that by including product resellers or vendors, who have no direct or indirect control of these areas, misapplication of the procurement language in this Standard would impose unrealistic obligations, standards of care, and potential liability on professional services related to the supply chain. As a consequence, services currently provided by	

engineering firms may be uninsurable under current professional liability insurance policies. Other industries supporting the supply chain have raised similar concerns, noting that the effect of this approach will be to stifle competition, impair innovation, and increase costs.

Specifically, the guidance language in this Standard includes "integrator" requirements that impose responsibilities on engineering firms and other supply chain elements for control of software development; personnel management systems; industrial system controls (SCADA); and long- term or post-contract reporting/remediation requirements (vulnerability testing and mitigation). Engineering firms do not typically develop such software and hardware, yet the guidance language suggests they should assume such liability for their use. They also do not monitor and report vulnerabilities for vendor software and hardware. This "one-size-fits-all" approach amounts to a significant reallocation of risk, imposing liability on engineering firms that they can neither manage, nor price. The result will be fewer firms willing to perform services for this industry. This requirement should be modified to limit the scope and responsibilities to the vendor and end user to ensure risk is apportioned to the responsible parties.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

Requirement R1 requires a documented ‘supply chain risk management plan’, AZPS requests clarification and renaming of the plan to ‘vendor risk management plan’ throughout the Standard as this term more appropriately describes the content that is required to be included in the plan. Also, the statement …’the plan(s) shall address:’ seems redundant and potentially creates a distinction that is not intended. AZPS recommends striking the last sentence and appending …’including’ to the first sentence of Requirement R1. Finally, AZPS recommends revising the language of Requirement R1 to focus on BES Cyber Systems and to allow the plan content to address when the associated “Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets” are brought into the scope of such plans as follows:

R1. Each Responsible Entity shall implement one or more documented ***Vendor*** risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems, ***including***: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. The use of controls in BES Cyber System planning and development to:

1.1.1. Identify and assess risk(s) during the procurement and deployment of vendor products and services; and

1.1.2. Evaluate methods to address identified risk(s).

1.2. The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems:

1.2.1. Process(es) for notification of vendor security events;

1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3. Process(es) for disclosure of known vulnerabilities;

1.2.4. Coordination of response to vendor-related cyber security incidents;

1.2.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

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

1.2.7. Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

1.3. The applicability of controls to associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

AZPS also requests that two (2) definitions utilized in the Technical Guidance and Examples be proposed for inclusion as defined terms in the standard, "Security Events" and "Vendor." Specifically, AZPS notes that Requirement R1.2.1 uses the term "security events" as an undefined term in the Standard, but that the Technical Guidance and Examples, Page 6, uses "Security Events" as a defined term. AZPS requests consistency between the two documents and the addition of the defined term "Security Events" to the Standard. Additionally, AZPS requests the removal of 'identified, threatened, attempted' from the defined term and require only notification of 'successful breach of vendor's components, software or systems that have potential adverse impacts to the availability or reliability of BES Cyber Systems'. Further, the Rationale for Requirement R1 defines the term "vendors" as '(i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators', AZPS requests incorporating this definition in the Standard for specificity of scope.

AZPS requests clarification regarding the term "processes" as used in Requirement R1.2. In particular, AZPS requests clarification that these items or "processes" are to be included in the overall plan and do not require a separate process or process documentation. Finally, the Rationale for Requirement R1 states that "obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement the Entity's plan;" however the Requirement does not make clear that the failure of contract negotiations to result in specific controls would not be considered a failure to implement.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG agrees with the intent of this requirement, but has the following questions/recommendations below:

- The term vendors as used in the standards is defined in the Rationale for Requirement R1 box. This term should be officially defined in the Glossary of Terms used in NERC Reliability Standards.

- Is requirement R1 applicable to new additions and/or modifications to existing BES Cyber Systems? There is not sufficient information to determine if this requirement is applicable only to new BES Cyber Systems or if it also includes changes to existing BES Cyber Systems.

- The applicability of Requirement R1 to High/Medium/Low BES Cyber systems and EACMs, PACs and PCAs is not clear the way it is written. Recommend using the applicability tables as in CIP-004 through CIP-011 for the requirements in this standard, especially R1.

- Requirements 1.2.1 through 1.2.6 discuss processes for vendor controls but some of the controls are unclear as to who is expected to perform the “notification”. For each sub-requirement, PSEG recommends adding clarity in the requirement language indicating who is expected to perform the notification, the vendor or the registered entity.

- Requirement 1.2.1 discusses a vendor security event. This is a vague term. The standard should include more clarification on what a vendor security event is or define the term.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern Company strongly encourages the SDT to consider the below edits, which use phrasing directly from the FERC Order. If R1 is intended to address the true supply chain procurement side of things, then the proposed edits provided below appropriately scope this requirement at the ‘main R’ level. The Order 829 Summary, and paragraphs 10 and 24 of the Order specify controls for vendors that supply “industrial control systems” products and services. Therefore, R1 should be focused on to what vendors and what software/firmware this requirement should be limited. The expansion of scope at this stage to propose including all impact classifications of BES Cyber Systems and their associated EACMS, PACS, and PCAs is above and beyond the Order, in our opinion. It’s absolutely unmanageable if not restricted somehow to higher level systems. In CIP audits, “BES Cyber Systems” immediately turn into a list of hundreds or thousands of "programmable electronic devices."

The proposed edits provided below move the “planning and procurement” phases of the lifecycle up from sub-requirements 1.1 and 1.1.1 to the main requirement so that all of the sub-requirements under R1 are appropriately scoped as well. Without this, for example, R1.2 applies to all risks at all times throughout the entire lifecycle of all devices. It’s cleaner to have the ‘main R’ be about the plan and setting the scope of the plan, and then have the sub-requirements address the plan(s) specifics. Consistent with Order 829, language from the rationale section addressing the “forward-looking” nature of this new requirement(s) has been incorporated into the main R1 requirement itself. Modifications highlighted below in R1.2.5 are recommended to eliminate redundancy and avoid confusion, while also addressing the specifics in the Order for dealing with “cyber incidents.” The order of the sub-requirements of R1.2 have also been adjusted to more clearly align with the planning and procurement life-cycle, while at the same time continuing to address directives in the Order.

Additionally, Southern Company agrees with comments submitted by Georgia Transmission Corporation (GTC), specifically with regard to defining the term “Supply Chain” in accordance with the Order-referenced NIST 800-53 defined term which establishes the applicable time horizon for this Standard, and removal of references to Electronic Access Control and Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Modify the R1 language as follows:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating planning and procurement cyber security risks for industrial control system vendor products and services used in BES Cyber Systems. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts. The plan(s) shall address: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Process(es) for the identification and assessment of risk(s) *of industrial control system vendor products and services*.

1.2 Methods to evaluate controls to address identified risk(s) in R1.1, that includes the following:

1.2.1 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s);

1.2.2 Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3 Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

1.2.4 Process(es) for disclosure of known vulnerabilities in vendor products;

1.2.5 Process(es) for notification of and coordination of response to vendor-related cyber security incidents; and

1.2.6 Other process(es) to address risk(s) as determined in Part 1.1, if applicable.

Likes 0	
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	

Jeanie Doty - Austin Energy - 5	
Answer	
Document Name	
Comment	
For all Questions - I support the comments of Andrew Gallo, Austin Energy	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
The draft Requirement R1.2 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R1.2, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless a vendor agrees to notify the Responsible Entity of vendor-identified vulnerabilities in the Cyber Assets provided or maintained by the vendor, Responsible Entities cannot comply with R1.2.3. Responsible Entities could encounter scenarios where: • Vendors may refuse to comply with the Responsible Entity’s vendor controls; • Vendors may demand an unreasonably high payment for compliance with the Responsible Entity’s vendor controls; • Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or	

• Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance “safety valve” is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity’s required controls. Such a “safety valve” would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that “[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan.”

Guidance language in the G&TB portion of a Standard is helpful, but the “safety valve” concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary “safety valve” along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

The Rational for Requirement R2 lists several sources for supply chain vulnerabilities, but it is not clear what is considered a relevant source and whether the entity is required to review all sources of supply chain vulnerabilities which may be very burdensome. CenterPoint Energy recommends adding the specific sources of vulnerability information, such as E-ISAC or ICS-CERT in the requirement.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

2) For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

3) Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.
2. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.
3. Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

4. SDT should clarify that existing contracts do not need to be renegotiated based on the 15-calendar month reassessment of the plan or other plan revisions.

5. Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends that each requirement should have a provision for allows an entity to accept the risk of selection a vendor that will not or cannot supply a control. NRG recommends removal of R2.1 language which is covered in R2.

For R2, will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? This seems to imply scope creep from elements on R1. Is “necessity” defined by entity, NERC, or outside source?

NRG requests clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Dominion recommends that requirement R2 be replaced with the following:

“Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 related to procuring and installing unsecure equipment or software, the risk of unintentionally failing to anticipate security issues that may arise due to network architecture, unintentionally arise during technology and vendor transitions, and purchasing software that is counterfeit or that has been modified by an unauthorized party at least once every 15 calendar months, which shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]”*

Dominion is of the opinion that the activities specified in Part 2.1 are included in the language of R2. Dominion recommends modifying Part 2.1 and 2.2 as follows:

- 2.1 Revision(s), if any, to address applicable new supply chain security risks that include security considerations related to cyber security, and
- 2.2 The supply chain plan(s) shall be reviewed, updated as necessary, and approved by CIP SM or delegate at least once every fifteen (15) months.

Also see the recommendation for replacing this requirement as described in the comments for R1.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

Refer to our comments on R1.

We do not agree with the approach in R1 (and R2) of creating “plans” and the intent of the plans to “cover the procurement aspects of all four objectives.”

Order 829’s four objectives did not include creating “plans.” All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011.

NERC’s Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets.

With respect to R2 as proposed, 1,398 entities would have to annually research information, including information which is readily available to be proactively provided by NERC to them. This diverts and dilutes registered entities’ resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response
Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

Exelon feels that the R2.1 language is vague and has the potential to become administratively burdensome without a corresponding benefit to BES reliability. While Exelon agrees with the rationale that examples of sources of information that an entity could consider include guidance or information issued by the E-ISAC, this language should be included in the Requirement itself because only that language forms the basis of a compliance assessment. Exelon receives over 100 security-related messages regarding potential vulnerabilities per day from a myriad of sources. Without creating bounds around the sources to be considered as well as the periodicity for updates to supply chain cyber security risk management plan(s), the question of whether any or all of the messages should have been considered will be difficult, if not impossible, to evidence. Exelon points out that the E-ISAC already performs important filtering functions for the industry. Perhaps future Alerts issued by the E-ISAC could be enhanced to point out vulnerabilities that would require new mitigating controls in supply chain cyber security risk management plan(s). Without these limitations, each entity will need to develop processes and procedures to receive and filter information, define mitigating controls, update the plan(s) and obtain approvals which is inefficient at best and impossible to evidence at worst.

Further, Exelon suggests that while multiple updates to the plan(s) may occur within a year as new E-ISAC Alerts are issued, CIP Senior Manager Review and Approval should only be required every 15 months. Intermediate reviews and approvals, or reviews for minor changes, should be outside the scope of the Requirement.

Likes 0	
Dislikes 0	

Response
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We suggest moving this Requirement language to the CIP-003 Standard. Our group feels that CIP-003 is the most appropriate Standard to handle this Requirement which is applicable to Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response
Nicholas Lauriat - Network and Security Technologies - 1

Answer	No

Document Name	
Comment	
Approval of CIP Senior Manager or delegate should be required for both or neither of R1 and R2.	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See comments on Requirement R2 in attached file.	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	
Comment	

Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013.

The language of R2.1 appears redundant and not any different than what is already required in the language of the main requirement, R2. Suggest deleting R2.1.

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1

Answer	No
Document Name	

Comment

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4

Answer	No
Document Name	

Comment
• As previously stated, for consistency with other CIP Standards (e.g. Physical Security plans, Incident Response Plan, Recovery Plans, Information Protection program, etc..) , CIP-003 R1.1 should be expanded to include the Supply Chain Risk Management plan as part of the collective cyber security policies reviewed and approved by the CIP Sr. Manager at least every 15 months. And, applicability of supply chain risk management controls to assets that contain Low Impact BCS should be consigned to CIP-003, R1.2 and R2. • The NERC Glossary of Terms definition of CIP Senior Manager will require update to include CIP-013

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment
We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment
R2 contains the language “As necessary… at least once every 15 months…” Is it an “as necessary” requirement or is it once per 15 months? Recommend removing the “as necessary” language as it is too subjective and open to interpretation.

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	No

Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

1. Suggest deleting R2.1. The R2 language includes “review and update as necessary”. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.
2. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.
3. Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	
Response	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	

Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI supports the following comment from AEP: “R2 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R2 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R2 should be rewritten to be only applicable to high and medium impact BES Cyber Systems.”	
Likes 0	
Dislikes 0	
Response	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
R2 has no stated applicability and it is unclear whether the CIP Senior Manager approval required here is any different from the required approval under R5. It would be clearer if R2 were made into R1.3, with the clarification suggested in our comments above to clearly exclude Low BES Cyber Assets from this requirement and consolidate requirements for those assets under R5.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
What is the target of the word “revisions” at the beginning of R2.1? Does revisions refer to modifications of the “supply chain cyber security risk management plan(s)” document itself? If so, then requirement is redundant in that R2, and consequently R2.1 could be interpreted to require entities to evaluate the revisions that were just completed. Or is the intent of “revisions” to direct REs to consult document(s) external to the standard when executing revisions?	
Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.	

Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
R2 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R2 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R2 should be be rewritten to be only applicable to high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

R2 – first line – for clarity purposes NRECA recommends removing “and update, as necessary.”

R2.1 – strongly recommend deleting “to address applicable new supply chain security risks and mitigation measures” as it is unclear and unnecessarily open-ended.

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

SVP agrees with other entity comments that "additional evaluation of the revisions is an administrative task that does not enhance BES security."

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Concur with EEI’s Position	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months and removed from CIP-013-1.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute’s comments to Question 2.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

The way the Requirement is written once again leaves the Requirement open to interpretation.

The current text reads:

“Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include:”

SunPower believes the correct statement of R2 should read:

“Each Responsible Entity shall review, as necessary, but at least once every 15 calendar months, its supply chain cyber security risk management plan(s) specified in Requirement R1 and update as necessary. The reviews and updates includes, but not limited to:”

SunPower also believes that the intent of R2.1 is not clear when the Requirement states, “to address applicable new . . . “ SunPower believes the term “applicable” needs to be left out of the Requirement unless the SDT is talking to the Applicability Section of the Standard, if that is the case, then state the Applicability Section. If that is not the case, SunPower believes the sub part should read:

“2.1 Evaluation of revisions, if any to address newly identified supply chain security risks and mitigation measures”

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We generally agree with EEI’s comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

Agree that it is appropriate to reassess the Entity plan associated with R1.1, but updates to the R1.2 portion would be unmanageable to point of being non-productive for entities and suppliers, for the reasons already stated in the R1 response above.

Likes 0	
Dislikes 0	
Response	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
The annual assessment of new risk is too open ended for a mandatory and enforceable Standard.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	
1) Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.	

2) For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

3) Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

SDT should clarify that existing contracts do not need to be renegotiated based on the 15-calendar month reassessment of the plan or other plan revisions.

Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

It is not clear if the approval by the CIP Senior Manager is required with the first version of the plans, or only for subsequent revisions. It is not clear if the approval by the CIP Senior Manager or delegate is required with each review cycle or only if modifications are made to the document(s).

Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Agree that it is appropriate to reassess the Entity plan associated with R1.1. For the reasons already stated in the R1 response, updates to the R1.2 requirements would be unmanageable to point of being non-productive for entities and suppliers.	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC knows of no definitive source to identify “new supply chain security risks and mitigation measures.” Therefore, compliance with this requirement part becomes subjective thus is not auditable. Reviewing and updating the plan as necessary under the core R2 along with CIP Senior Manager approval per R2.2 should be sufficient to maintaining a quality cyber security supply chain risk management program. We recommend the removal of requirement part 2.1.	

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

We feel that there should be some guidance on where to look for "emerging supply chain related concerns". If our company is using a particular source and miss a notification on another site, will we be penalized?

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

With regards to the periodic reassessment of supply chain cyber security risk management controls, the IRC and SWG request the SDT provide objective criteria for the scope and content of the review to ensure consistent implementation against set criteria. Does this only require update of the plan document? Do needed contract revisions have to be documented? What is required to demonstrate review and consideration of items that may not be incorporated into the updated plan?

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

We feel that there should be some guidance on where to look for "emerging supply chain related concerns". If our company is using a particular source and miss a notification on another site, will we be penalized?

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language. R2 needs a more clear description on when mitigation measures are required. For example, would the selection of one vendor over another be considered a mitigation measure? Would an entity be required to always choose the vendor with the best-in-class security posture despite cost?

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
We believe that sub requirements (2.1 and 2.2) in R2 are unnecessary. Similar verbiage used in CIP-003-6 for review of cyber security policy can be used in this instance. Also, can the CIP Senior Manager delegate this accountability?	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	

Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
With regards to the periodic reassessment of supply chain cyber security risk management controls, the IESO request the SDT provide objective criteria for the scope and content of the review to ensure consistent implementation against set criteria. Does this only require update of the plan document? Do needed ntract revisions have to be documented? What is required to demonstrate review and consideration of items that may not be incorporated into the updated plan?

Likes 0	
Dislikes 0	

Response

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	

Comment
This should be removed and convered in CIP-003.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	

Comment
1) Suggest deleting R2.1. The R2 language includes “review and update as necessary”. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

Likes 0	

Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA believes if the scope and language for R1 is appropriate, the review process is necessary but should not require CIP Senior Manager Approval. BPA suggests maintaining consistency across standards: CIP Senior Manager approval is required for policies rather than plans.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
R2 IPC suggests the SDT consider re-structuring the proposed format for R2 to align with current enforceable standard format (see CIP-002-5.1 R2, R2.1, and R2.2): The Responsible Entity shall: (1) Review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, (2) Evaluate revisions, if any, to address applicable new supply chain security risks and mitigation measures; and (Question) How does the SDT foresee this evaluation being measured and accomplished? (3) Obtain its CIP Senior Manager or delegate approval (Question) Is the CIP Senior Manager or delegate intended to be an approval of the plan every 15 months? If so, IPC recommends specifying the timing and what is being approved in the wording of the requirement. IPC does not believe R2.2 provides any security measures or controls and is simply an administrative exercise. IPC recommends R2.2 be removed.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	
Comment	

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

Reclamation recommends Requirement R2 should instead require entities to implement their supply chain risk management plan(s) developed in Requirement R1.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	
Response	

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	No
Document Name	
Comment	

1. Requiring a greater level of testing, documentation, or security features from system integrators, suppliers, and external service providers may increase the price of a product or service, and increase the compliance burden for the industry. We recommend language addressing key questions, such as: at what time frame does the risk reduce to acceptable: Daily, weekly, monthly or yearly? How is the standard addressing acceptance of risk?

Likes 0	
Dislikes 0	
Response	

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	
Comment	

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

While it is not unreasonable to propose periodic review and reassessment to assure some minimum level of rigor, ultimately Registered Entities know that plans are living documents that must be supported by sound security practices implemented to stay apprised of emerging cybersecurity threats as they enter the landscape, and a 15-month reassessment is ill-equipped to support the pace of the ever-evolving threat landscape. The industry might be better served with language that supports a periodic review coupled with the need for ongoing and timely assessment and update of plans on an as needed basis when the impending threat warrants the action.

The SDT may want to reconsider the need and intended value for CIP Senior Manager approval for these reasons. 1.) While it is not unreasonable to propose an approval for plans of this nature, prescribing this as a CIP Senior Manager responsibility is inconsistent with other enforceable mandatory CIP Cyber Security Reliability Standards that limit these approvals to BES Cyber System populations, policy, and, exceptions (both CIP Exceptional Circumstances and Technical Feasibility Exceptions). 2.) The introduction of CIP Senior Manager or delegate approval may not provide the intended value for the complex range of jurisdictional, technical, economic, and business relationship issues. 3.) By NERC definition, as a technicality, please note that the scope of the CIP Senior Manager accountabilities is currently prescribed as CIP-002 – CIP-011 and would require amendment. 4.) Lastly, as a consideration, the SDT may want to revisit the need for this level of approval and to align the approach with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	

1. Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

1. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

SDT should clarify that existing contracts do not need to be renegotiated based on the 15 calendar month reassessment of the plan or other plan revisions.

An entity’s plan must be implemented at the commencement of negotiations.

Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	

Comment

R2 is pretty straightforward, however unless modified by a subsequent implementation plan, WECC would expect an entity to have a reviewed and approved SCRM plan on or before the effective date, then complete R2 on intervals of no more than 15 calendar months. If an entity exceeds the 15 calendar month time frame, an R2 PNC would be indicated.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment
SRP agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, SRP requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	

Comment
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
While supporting this requirement, ACEC recommends that the requirement be modified to state it only applies to high and medium impact, consistent with requirements R3 and R4.

Likes 0	

Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	

AE agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, AE requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

PRPA agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, PRPA requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	Yes
Document Name	

Comment

CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	Yes
Document Name	
Comment	

Duke Energy suggests the drafting team consider collapsing 2.1 and 2.2 into one sub-requirement. We do not see the need in having these as two sub-requirements, and this would mirror the language used in CIP-003-6.

Also, the use of the term “applicable” in R2.1, appears vague and could lead to potential disagreement on what supply chain security issues actually pose a substantial risk.

Likes 0	
Dislikes 0	
Response	

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	Yes
Document Name	
Comment	

Proposed CIP-013-1, R2 properly implements Order No. 829’s directive to develop a Standard requiring entities to periodically review and approve the controls adopted to address specific security objectives associated with supply chain risk management.

Likes 0	
Dislikes 0	
Response	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	Yes
Document Name	
Comment	

No additional comments.

Likes 0	
Dislikes 0	
Response	

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The use of 15 calendar months allows entities to review and update (as required) on a systematic basis, the same time every year, Thank you.	
Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company strongly encourages the SDT to consider the below edits to R2 to make it clear that assessment of risks and revisions to the plan are required on a “once every 15 months” interval, and not at the time of each and every notification of any new potential risks/vulnerability. The below proposed modifications also clarify that *revisions* to the plan(s) are predicated on the existence of “new supply chain cyber security risks” by moving the phrase “if any.” Subsequently, R2.2 has been modified to require CIP Senior Manager or delegate approval only when, following a required review every 15 months, it is determined revisions to the plan(s) are warranted to address “new supply chain cyber security risks” or “mitigation measures.” As written in the draft Standard, an annual review and approval by the CIP Senior Manager or delegate where no revisions were warranted or made is a documentation exercise that provides no benefit to reliability or reduction of supply chain risk. The SDT should also consider strengthening the language in the Rationale and/or Guidelines directing Entities to adequate and/or designated sources (NERC/DHS/E-ISAC/ICS-CERT) providing Supply Chain guidance for those higher level issues that warrant a change to your plan(s). Also of note and for SDT consideration is the structure of the Implementation Plan for this Standard that does not require the CIP Senior Manager or delegate to review and approve the initial plan(s) on or before the effective date the plan(s) is required to be in place; therefore, review and approval of the plan(s) would be 15 months after the plan(s) was already in effect.

Modify R2 language as follows:

R2. Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in Requirement R1 and update them, as necessary, at least once every 15 calendar months, which shall include:

2.1. Evaluation of revisions to address new supply chain cyber security risks and mitigation measures, if any, related to industrial control system vendor products and services applicable to the Responsible Entity’s BES Cyber Cyber Systems; and

2.2. Obtaining CIP Senior Manager or delegate approval for any revisions to the plan(s).

Likes 0	

Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment
ERCOT supports the IRC comments on this question.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	

Comment
Generally, we agree with the requirement to have the CIP Senior Manager review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. However, R2.1 could be interpreted in many ways that might introduce uncertainty in the process. In agreement with EEI, we suggest the following language: R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	

Comment
Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, SMUD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	

Comment

Seattle City Light agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Seattle City Light requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities (CSU) agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CSU requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures	
Likes 0	
Dislikes 0	
Response	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • Recommend changing Requirement 2.1 from “Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and” to “Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures as determined by the registered entity; and”. • The standard language does not address how a revision to the plan needs to be addressed by contracts already in process/negotiation at the time of review or revision. Please provide guidance.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

For consistency and to ensure that the requirement appropriately reflects the scope of risks being addressed, AZPS requests striking of ‘supply chain security risks’ in Requirement R2.1 and replacing with ‘Vendor security risks’.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	Yes
Document Name	

Comment

Santee Cooper agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Santee Cooper requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	Yes
Document Name	

Comment

OUC agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, OUC requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	
Document Name	

Comment

CPS Energy supports the comments provided by APPA

Likes 0	
Dislikes 0	
Response	

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	No
Document Name	

Comment

Suggest “software, firmware, and associated patches” Possible TFE language for R3? The

NSRF recommends the following:

Q 3. Add language to address potential Technical Feasibility Exception (TFE).

R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware**, where technically feasible,** before being placed in operation on high and medium impact BES Cyber Systems:

R3.2

“Firmware” is already included in R3 this redundant in R3.2 recommend R3 to be written as a general Requirement with specifics in the sub Requirements.

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn’t clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	

TFE opportunity is again needed, especially to address vendor-proprietary (“black box”) vendor software and firmware, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses).

R1.2.5 is largely duplicative of R3. They should be made consistent, or one of them should be deleted.

R3 may better belong in CIP-007 and needs to be aligned with CIP-010. Requirements for a single topic should be consolidated within a single standard.

Likes 0	
Dislikes 0	
Response	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	

See APPA's, TAP's, and USI's comments.

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	
Response	

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

It may not be possible to verify the integrity and authenticity of software and firmware before being placed into operation if the Vendor is no longer in business or will not cooperate. There should either be an exception or ‘*out’* for possibility (e.g. … where possible.), leaving that determination up to an audit team, or a feasibility exception should be allowed.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Change/add language to emphasize that failure to obtain the cyber security controls from a vendor doesn't translate to being out of compliance. Entity should have the ability to mitigate risks posed by vendors. Furthermore, this risk should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-007 R2.

IID feels that there should be an exclusion or exception (similar to a CIP Exceptional Circumstance or Technical Feasibility Exception) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Would deployment tools that rely on digital signature enforcement (such as Microsoft Authenticode Security Verification or Red Hat signature verification) satisfy the intent of this requirement where such mechanisms provide technical checks for verification of authenticity and integrity?

The requirement measures should allow automated deployment tools such as Microsoft's System Center Configuration Management to be trusted for the purpose of confirming the integrity and authenticity of software and firmware.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy recommends the following language revision to R3.

"For BES Cyber Systems in production, each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware prior to installation on high and medium impact BES Cyber Systems:"

We suggest the addition of the phrase "For BES Cyber Systems in production," at the outset of the requirement.

We also recommend replacing the phrase "placed in operation" with "prior to installation" in R3. The phrase "placed in operation" is ambiguous, and could be open to debate as to what this actually means. The language "prior to installation" is less ambiguous, the language used in FERC Order 829, and is already used in the rationale section for this requirement.

Also, Duke Energy has some concern with the amount of involvement/cooperation that will be necessary from a vendor in order to achieve compliance with this requirement. Some issues may arise if/when a vendor is not able to verify the integrity or authenticity of a certain product. We suggest the drafting team consider this situation as appropriate for a Technical Feasibility Exception or in some instances be granted a CIP Exceptional Circumstance. For example, an issue could arise wherein an entity has a device that is failing, and a fix (update of software) is needed immediately. In the interest of system stability, there may not be enough time to wait on a vendor to send a certificate of authenticity on a patch or software upgrade. We feel that a Technical Feasibility Exception and CIP Exceptional Circumstance should be considered based on these issues.

Another aspect of R3 that we think requires some clarity is whether or not R3 should apply at the BES Cyber Asset level. Currently, the language explicitly states BES Cyber System, but we feel that the language may not represent the actual intent of the requirement. If the controls proposed in R3 are better suited at the Cyber Asset level, the language should be revised to reflect this.

Lastly, Duke Energy would like to suggest that the drafting team consider that this requirement be moved to current standard CIP-007-6. CIP-007-6 already addresses security controls for BES Cyber Systems, and we feel that this control oriented requirement may be better suited there.

Likes 0	
Dislikes 0	
Response	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Requirement R3 mentions high and medium BES Cyber Systems, but does not include their associated Electronic Access Control and Monitoring Systems (EACMs), Physical Access Controls(PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following modifications for consideration:

1. R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems [and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets]:

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

CIP-007 R2 requires a mitigation plan for patches that cannot be applied within 35 days. Please confirm that if a patch cannot be applied within 35 days due to the vendor's inability to provide the integrity check, there is no other compliance risk if the RE provides a mitigation plan in accordance with CIP-007 R2.

Additionally, if vendors refuse or can't provide hashes or other verification methods, please provide confirmation that an internal process to test, scan and perform verification activities would be enough to satisfy this requirement.

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC comments.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI urges the SDT to remove R3 and address firmware and software integrity/authenticity in the supply chain risk management plan(s) as detailed in the requirement concepts proposed by AECI in Question 1. This will allow Responsible Entities to address this issue contractually with applicable vendors in the supply chain/procurement process and not the operational time horizon.	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	

Answer	No
Document Name	
Comment	
PRPA requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	
AE requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No

Document Name	

Comment

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business or will not cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date.

3. The applicability of this requirement should be limited to high and medium impact BES Cyber Systems with external routable connectivity. This would align the standard with the applicability of CIP-007 and CIP-010.

4. Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

5. Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

6. Provide clarity for when a system is pre-loaded by a vendor and delivered to an entity. Is the entity required to verify software authenticity? If a computer is purchased from Dell, can Dell provide authenticity for all of the firm ware that is part of the system but not directly manufactured by Dell; i.e. system bios, sound system, network adapter, video controller.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
This requirement should be incorporated into CIP-007 R2 or CIP-010 R1. This is a System Security Management requirement and belongs in the appropriate location. CIP-013-1 R3.1-R3.4 are all components of the the CIP-010 baseline. Placing this topic in a separate standard and requirement creates compliance confusion. As entities will have to follow different requirements in CIP-007, CIP-010, and CIP-013, there is an increased likelihood of a violation. As there is no consistency within the software industry on the use of hash functions, there must be guidelines on what is considered an acceptable approach to meet this requirement. While guidelines are needed, it must be understood that many times the individual utility has little influence on software vendors due to the relatively small purchasing power of the electric sector relative to the vendor's overall market.	
Likes 0	

Dislikes 0	
Response	
Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	

Comment

- The scope of CIP-013-1 R3 overlaps with parts of CIP-007-6 R2 and CIP-010-2 R1.1-1.5. However, both CIP-007 R2 and CIP-010 R1 apply to High and Medium BCS and associated EACMS, PACs, and PCAs. The potential collision of requirements that apply inconsistently (e.g. BCS vs EACMS) across three standards will be difficult to manage, monitor, and implement. For example, timing of security patch implementation per CIP-007 R2.3 could be impeded by authenticity processes required in CIP-013. Meeting compliance with CIP-013 could unintentionally cause not only potential compliance problems with CIP-007 R2, but also significant security, operational, and/or reliability impacts.
- An exception process is required for R3. This requirement will apply to the existing complement of High and Medium BCS, upon the enforcement date of the new Standard. However, since entities are explicitly not required to renegotiate existing contracts, it may be difficult to meet compliance with this requirement upon enforcement, if existing vendors do not provide appropriate support.
- Measures and Evidence – Since the R3 requires an entity to show that documented processes have been implemented, M1 does not adequately describe the evidence required to demonstrate implementation.

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	

Comment
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	

Comment

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.
2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations.

Does R3 allow the Entity to “accept the risk?”

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R3. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5 we suggest adding the language “subject to procurement contract.”

To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.” There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

Additionally, R3 may hinder an entity’s ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan”

We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?

Likes 0	
Dislikes 0	

Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See comments n Requirement R3 in attached file.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST strongly supports the goal of verifying software integrity and authenticity and hopes vendors will be generally willing to provide Responsible Entities with checksums, cyber hash values, or other integrity checks for their software and firmware. However, as written the requirement creates the potential for a conflict with CIP-007-6 R2 Part 2.3 (installation of applicable security updates), and could leave a Responsible Entity with potentially no recourse other than to create a mitigation plan if a vendor is for some reason unable or unwilling to provide such integrity verification for a patch or other type of software or firmware update. N&ST recommends that the SDT consider allowing for exceptions that must be (a) fully documented and (b) approved by the Responsible Entity's CIP Senior Manager	
Likes 0	

Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	

Comment

We agree with the drafting team that verification to the integrity and authenticity of the software needs to be validated. However, we would ask the question, “If the industry finds validations issues, how do we hold the vendor accountable?” We understand that contracts are in place to help this situation, but this doesn’t always resolve validation issues. We feel that FERC Order 829 language falls short of holding the vendors accountable in reference to addressing verification of software integrity and authenticity and as a result, the compliance burden is placed on the users. The CIP requirements focus on the Responsible Entity carrying the compliance risk even if the industry can identify vendor validation issues. For example, entities could potentially pay for product upgrades to address compliance concerns when it’s been verified that the current product upgrades have not met the quality of service that was promised by the vendor. We suggest that the drafting team hold open discussions with FERC, potentially conducting a gap analysis in reference to this potential concern. If the analysis determines a gap, FERC should seek legislation to hold vendors more accountable.

Also, we suggest that Requirement R3 language should be moved to the CIP-010 Standard. Our group feels that the CIP-010 Standard adequately addresses software and firmware verification. Additionally, we propose some language revisions to the Requirement language.

SPP’s proposed language revision to R3:

“Each Responsible Entity shall implement one or more documented process for verifying the integrity and authenticity of the following software and firmware before being installed in operation on high and medium impact BES Cyber Systems”.

The term “installed” has been consistently used throughout the CIP-010 Standard and we feel this will give our proposed language validity and consistency.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

The draft Requirement R3 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R3 compliance, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless the vendor agrees to cooperate with any software integrity and authenticity verification process, the Responsible Entity will be unable to ensure the integrity and authenticity of software used in covered Cyber Assets.

Responsible Entities could encounter scenarios where:

• Vendors may refuse to comply with the Responsible Entity's vendor controls;

• Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;

• Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or

- Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's required controls. Such a "safety valve" would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Guidance language in the G&TB portion of a Standard is helpful, but the "safety valve" concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary "safety valve" along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

Exelon does not support the draft language in R3 which requires an Entity to verify the integrity and authenticity before placing a BES Cyber System into operation. Instead, Exelon prefers the suggested language from Order No. 829 that directs "the integrity of the software and patches before they are installed in the BES Cyber System environment" (P. 48). Accordingly, Exelon suggests that R3 be edited to read as follows:

Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware **prior to installation into** high and medium impact BES Cyber Systems

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that for future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

Specific operational cyber security controls are best addressed as revisions to CIP-002 through -011.

Prescribing verification of integrity and authenticity is a “how” not a “what.”

Refer to EEI comments on R3. We agree with the concept of the EEI comments to consider a revision in CIP-010 for a specific security objective (“what”), such as “method(s) to minimize the risk of installing compromised” CIP-010 R1 baseline configuration items.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Patch Management obligations for cyber security related patches are already addressed in CIP-007. Dominion is of the opinion that the obligations in this requirement would be better placed (once it's determined what the obligations should be) in CIP-010 or CIP-007.
- If R3 is kept in CIP-013 and not moved to an existing CIP Standard, we recommend the following:

R3: Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following, prior to authorized installation on high and medium impact BES Cyber Systems and associated EACMSs, PCAs, and PACs: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

SCE&G agrees with the concerns and questions raised by the Edison Electric Institute (EEI), including the following:

"Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls. For example, the language could allow a Responsible Entity to use a vendor's website for verifying both integrity and authenticity, which will not protect against a Watering Hole attack, where the vendor's website has been compromised and both the

software and the integrity check are likely to be compromised. However, we note that the majority of vendors use their websites for software downloads and include the hashes for integrity checks on those websites. Members have had difficulty in getting vendors to change their practices, which makes this requirement difficult if not impossible for Responsible Entities to comply with…Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third part, a vendor."

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG recommends that the R3 and R4 technical/operation control requirements should be located in the associated standard to avoid misalignments or jeopardizing timeframes outline in the other standards such as patch management. For Example: R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4.

NRG requests clarification from SDT regarding what could/should an entity do if there is no process to verify the authenticity of software? In those cases, can an entity document their defense in depth strategies as a compensating measure? NRG recommends that SDT communicate in Measures that verification of authenticity could include a way to present in our processes other methods that may not actually be verification.

NRG recommends that SDT list ways that a Registered Entity can authenticate a source in the Measures section. NRG also recommends that SDT list that a Registered Entity should have a means to use putty, Debian, or things that don't have as tight of controls, (i.e. provide a checksum, and/or set a policy that they don't use open source code and requests clarification of how a Registered Entity would demonstrate that they had verified an authoritative source (i.e. open source) to the extent of what their capability would allow). For example, NRG recommends that SDT list examples in Measures section to include use of a layered approach of security and functional testing: For example start with a notification process, authenticity check of source, and use hash / checksum, then perform testing (but how does testing demonstrate authenticity? Answer – virus scan, etc (functional vs. security testing: A/V scan, logging, access, control). Lastly perform a scan from a vulnerability assessment tool. How does this prove integrity and authenticity of the software? NRG requests clarification in the standard requirement of when this requirement would become effective. NRG recommends that the SDT allow the Registered Entities additional time for vendor re-negotiations relating to supply chain for the purposes of enabling validation of integrity and authenticity of software and firmware.

NRG suggests that the R3 language should move to CIP-010. NRG requests clarification of whether testing is a valid form of verification. Additionally, we suggest the Requirement language to read as follows "Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being installed in operation on high and medium impact BES Cyber Systems". Each requirement should have a provision that allows an entity to accept the risk of selection a vendor that will not or cannot supply a control.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3. Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Does R3 allow the Entity to “accept the risk?”

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R3. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.” There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

4. Additionally, R3 may hinder an entity’s ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

5. Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan”

6. We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

SCE&G agrees with the concerns and questions raised by the Edison Electric Institute (EEI), including the following:

"Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls. For example, the language could allow a Responsible Entity to use a vendor's website for verifying both integrity and authenticity, which will not protect against a Watering Hole attack, where the vendor's website has been compromised and both the software and the integrity check are likely to be compromised. However, we note that the majority of vendors use their websites for software downloads and include the hashes for integrity checks on those websites. Members have had difficulty in getting vendors to change their practices, which makes this requirement difficult if not impossible for Responsible Entities to comply with…Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third part, a vendor."

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3) Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

R3 applies whether revised contract terms and conditions exist or not, with no exception for vendor capability issues, technical feasibility, or situations where there is no vendor. It is also not clear whether changes that are not firmware or software versions or patches fall under the requirement. CenterPoint Energy requests that the phrase “where technically feasible” be added to Requirement 3.

Furthermore, the Company believes verifying software integrity and authenticity as described in CIP-013 R3 belong in CIP-010 and recommends aligning the R3 sub-requirements to match the items in CIP-010 R1.

It is not clear what an entity must do if the vendor will not or cannot assist by providing an authentication method. Having a verification requirement for R3.4, where not automatically supported by vendors, slows down the existing patch management process. This increases security risks by leaving systems unpatched against known vulnerabilities for longer periods and increases compliance risks for entities where dated mitigation plans must be used to document delays.

Additionally, it is not clear whether secure boot capability, default on many Cyber Asset operating systems, is adequate (or even required) to demonstrate compliance with software verification requirement.

CenterPoint Energy recommends that R3 be revised for flexibility and feasibility. It should also be moved to CIP-010 as these requirements would seem to fit as a part of existing configuration change management processes.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	No
Document Name	

Comment

OUC requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

CIP-013-1 Requirement R3 is written with an assumption that the supplier provides a mechanism in which verification of integrity and authenticity can be performed on software and firmware. These tools/mechanism may not always be available to the Registered Entity, and the Registered Entity may not have the power in which to force the supplier to provide a verification method. Consistent with currently approved and enforceable CIP Cyber Security Reliability Standards, ATC recommends the SDT consider adding language to provision for conditions where it is not technically possible to perform a verification in order to provide the flexibility needed to preclude an impossibility of achieving compliance.

Additionally, the inclusion of "firmware" within the proposed language in CIP-013-1 R3 is an expansion in scope from the **first directive** in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard that "…should address the following security objectives, discussed in detail below: **(1) software integrity and authenticity;** (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

Additionally, CIP-013-1 Requirement R3 is simultaneously duplicative and additive with currently approved and enforceable CIP-010-2 Requirement R1 and the Applicable Systems within CIP-010-2 Requirement R1 Parts 1.1 – 1.5 as consequence of the broad reference to "high and medium impact BES Cyber Systems" without consideration of the construct of the CIP-010-2 Standard.

1. CIP-013-1 Requirement R3 Sub Requirements R3.1 – R3.4 are duplicative of CIP-010-2 Requirement R1 Parts 1.1 – 1.2, which obligates Registered Entities to develop and maintain a baseline of 'software' information for both high and medium impact BES Cyber Systems, where the types of software are effectively the same as what is being proposed.

    - CIP-010-2 Requirement R1 Part 1.5 addresses the testing of changes to this 'software' and 'firmware' for high impact BES Cyber Systems, rendering Sub Requirement R3.1 – R3.4 superfluous and unnecessary. Consequently, Requirement R3.1 – R3.4 also creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-010-2 Requirement R1 Part 1.5. In

its redundancy, it is at odds with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

- CIP-010-2 Requirement R1 Part 1.5 has a provision to allow for the testing of this software and firmware in production where it is not technically feasible to perform testing in a test environment. CIP-013-1 R3 is effectively an expansion in scope to CIP-010-2 Requirement R1 Part 1.5 in its obligation to perform testing "…**before being placed in operation on a high** … …**impact BES Cyber System**". Any expansion in scope to access requirements or controls for high impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-010-2 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

- CIP-010-2 Requirement R1 Part 1.5 is not applicable to medium impact BES Cyber Systems. CIP-013-1 R3 is effectively an expansion in scope to CIP-010-2 Requirement R1 Part 1.5 in its obligation to perform testing "…**before being placed in operation on a… …medium impact BES Cyber System**". Any expansion in scope to access requirements or controls for medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-010-2 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	

Comment

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	

Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

Reclamation recommends Requirement R3 should instead require entities to review and update as necessary their supply chain risk management plan(s) developed in Requirement R1 at least once every 15 months.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Rationale for Requirement R3:

The rationale language for R3 states, “The 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.” R1, R2, and the Rationale for Requirement R3 do not specify the impact classification (High, Medium and Low) when referencing the BES Cyber System. R3 specifically states the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems.” IPC would like know if the inconsistent impact classification references were intended or were an oversight by the SDT.

R3

The requirement language for R3 states, “before being placed in operation on high and medium impact BES Cyber Systems.” R1, R2, and the Rationale for Requirement R3 do not specify the impact classification (High, Medium and Low) when referencing the BES Cyber System. R3 specifically states the

impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems.” IPC would like know if the inconsistent impact classification references were intended or were an oversight by the SDT.

The requirement language for R3 states, “Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware." IPC is concerned that the SDT developed a standard that requires Responsible Entities to “verify the integrity and authenticity” of software and firmware of which Responsible Entities have no oversight or control over what each vendor provides.

IPC does not feel CIP-013-1 is an appropriate standard to address R3. IPC believes this requirement belongs in CIP-007-6 or CIP-010-2 as R3 is related to patching or configuration change management. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-007-6 and CIP-010-2 address testing and verification of changes controls, which are typically performed by technical staff as they test, implement, and update systems.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

LCRA supports ERCOT’s comments. CIP-013 R3 directly impacts baseline data and as such should be located within CIP-010.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
1) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business or will not cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. 2) The applicability of this requirement should be limited to high and medium impact BES Cyber Systems with external routable connectivity. This would align the standard with the applicability and risk-based approach of CIP-007 and CIP-010. 3) Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011. 4) Provide clarity for when a system is pre-loaded by a vendor and delivered to an entity. Is the entity required to verify software authenticity? If a computer is purchased from Dell, can Dell provide authenticity for all of the firm ware that is part of the system but not directly manufactured by Dell; i.e. system bios, sound system, network adapter, video controller.	
Likes 0	
Dislikes 0	
Response	

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	

See EEI comments

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	No
Document Name	

Comment

Colorado Springs Utilities (CSU) requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

Within the Rationale, the word “ensure” is inappropriate. Even good controls do not “ensure” a desired outcome. It should also state that “software being installed in the BES Cyber System was not modified or altered without the knowledge of the supplier AND the recipient or licensee. Consider replacement of “ensure” with “confirm”.

R1. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. To address these concern, The IESO request that the SDT consider the use of provisional language to protect Responsible Entities such as use of a TFE.

R1. The SDT should consider the use of “validate” instead of “verify” in this requirement.

R1. The SDT should address situations that are outside the usual upgrade and patch processes. This includes the obligations for signature updates, and where a vendor brings code onsite (binary or source code) that the entity is not allowed to review.

Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
Seattle City Light requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	

FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	
Comment	

Security Objective

Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	
Comment	

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language. Furthermore, operational checks to verify security controls are not adversely affected are covered in other CIP standards.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA supports ERCOT's comments. CIP-013 R3 directly impacts baseline data and as such should be located within CIP-010.	
Likes 0	
Dislikes 0	
Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.	

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

Within the Rationale, the word "ensure" is inappropriate. Even good controls do not "ensure" a desired outcome. It should also state that "software being installed in the BES Cyber System was not modified or altered without the knowledge of the supplier AND the recipient or licensee. Consider replacement of "ensure" with "confirm".

R1. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. To address these concern, The IRC and SWG request that the SDT consider the use of provisional language to protect Responsible Entities such as use of a TFE.

R1. The SDT should consider the use of “validate” instead of “verify” in this requirement.

R1. The SDT should address situations that are outside the usual upgrade and patch processes. This includes the obligations for signature updates, and where a vendor brings code onsite (binary or source code) that the entity is not allowed to review.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity’s capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC disagrees with the proposed requirement. CIP-013-1 R3 requires actions to be taken by the Responsible Entity that are outside of the supply chain context. Paragraph 45 of Order No. 829, specifies this objective of software integrity and authenticity should be applied to “The Plan” identified in the core directive in the context of addressing supply chain management risks. The SDT has chosen to identify controls in R3 that are executed only as part of the day-to-day management of BES Cyber Systems. These controls fail to effectively address the security objective of addressing software integrity and authenticity, will have minimal security value, are administratively burdensome on industry, and are inconsistent with the supply chain context. SAFECode’s (http://www.safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf) Software Integrity Control’s whitepaper outlines controls that effectively address software integrity and authenticity. Nearly all of these controls must be implemented by the vendor. As such, Responsible Entity’s should have the flexibility to require the vendor to provide software assurance through contractual means. Such as “supplier provides customer ways to differentiate genuine from counterfeit software”

Unfortunately, the SDT has not provided controls that effectively address software integrity and authenticity and has instead focused its control as demonstrated by the language in the measure on ensuring the “entity performed the actions.” In order to provide entities the flexibility to effectively address the security risks associated with the supply chain, we respectfully request that the SDT revise its draft standard to be more in line with the framework identified in FERC Order 829. Our recommendation, consistent with our response to question 1, is as follows

GTC recommends the SDT reconsider relocating the attributes of R3 in a manner that addresses the security objective to “The Plan” specified in R1 to align with the FERC Order. This would allow the Responsible Entity to handle contractually with the vendor i.e. “supplier provides customer ways to differentiate genuine from counterfeit software (such as digital signatures)”. Our recommendation is consistent with our response to question 1, which is summarized as follows:

See GTC’s comment for Question #1.

Upon close review of FERC's directives summarized beginning on paragraph 43 through paragraph 62, the Order essentially directs this new Standard as outlined:

Paragraphs 43 – 45:

R1: Develop a plan to include security controls for supply chain management that address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services which are intended to support Bulk Electric System operations; that include the following four specific security objectives in the context of addressing supply chain management risks:

R1.1 Security objective 3 (*information system planning*)

R1.2 Security objective 4 (*vendor risk management and procurement controls*)

R1.3 Security objective 1 (*software integrity and authenticity*)

R1.4 Security objective 2 (*vendor remote access*)

Paragraph 43:

R2: Implement the plan specified in R1 in a forward looking manner.

Paragraphs 46 - 47:

R3: Review and update, as necessary its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months

R3.1 Evaluation of revisions…

R3.2 Obtaining CIP Senior Manager or delegate approval.

Paragraphs 48 – 50:

FERC prescribes the various ways to address the first objective to the plan.

Paragraphs 51 – 55:

FERC prescribes the various ways to address the second objective to the plan.

Paragraphs 56 – 58:

FERC prescribes the various ways to address the third objective to the plan.

Paragraphs 59 – 62:

FERC prescribes the various ways to address the fourth objective to the plan.

FERC goes on to respond to comments on Existing CIP Reliability Standards, beginning with paragraph 71, “while we recognize that existing CIP Reliability Standards include requirements that address aspects of supply chain management, we determine that existing Reliability Standards do not adequately protect against supply chain risks that are within a responsible entity’s control. Specifically, we find that existing CIP Reliability Standards do not provide adequate protection for the four aspects of supply chain risk management that underlie the four objectives for a new or modified Reliability Standard discussed above.” FERC summary continues to focus on CIP-013-1 being limited to aspects of supply chain risk management.

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

The NERC Entity is the customer of the hardware supplier and software supplier, not the designer, manufacturer and developer of what is being procured. As such, the Entity can only clearly state what they want the hardware and software to do – at a high level, likely derived from what the vendor said there product could do, along with the expectation that the product will be “bug free”. But the Entity should not be expected to have the expertise and tools to “verify the integrity and authenticity of software and firmware”. Integrity and authenticity can only be assured by each link backwards in the Supply Chain, and collectively that will only happen if each link of the Supply Chain agrees to control their link. CIP-013 is not in a position to impose those controls on the entire Supply Chain, but only on the end customer - NERC Registered Entity. That said, software and firmware should be expected to be checked for proper "functionality" by the Registered Entity, per past CIP practice.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich

Answer	No
Document Name	

Comment

See comments submitted by Black Hills Corporation

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	
Comment	

This Standard, and therefore this Requirement needs to be squarely focused on the vendor product or service being procured and not on the categorization of a BES Cyber System. Requirement R3 should not be limited to High and Medium Impact BES Cyber Systems. A SEL-421 is a SEL-421 and the same risks of procurement, including firmware updates, apply to all SEL-421s impacted regardless of where they are deployed. Software/firmware updates are often acquired once and widely deployed. This is especially true in the substation environment where the exact same firmware release will be used to update Medium and Low Impact relays.

Likes 0	
Dislikes 0	
Response	

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	
Comment	

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra

Answer	No
Document Name	
Comment	

1) R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3) Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Does R3 allow the Entity to “accept the risk?”

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

· Request “per system capability” wording for R3. Not all vendors provide a “golden hash” or other mechanism to validate.

· To be consistent with not requiring R1.2.5 we suggest adding the language “subject to procurement contract.”

To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.” There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

Additionally, R3 may hinder an entity’s ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan”

We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?

Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6

Answer	No
Document Name	

Comment

For a smaller CIP applicable medium impact BES Cyber System, we apply between 5,000 and 7,000 patches a year. The only feasible means for us to apply any meaningful integrity check is through automated, cryptographic mechanisms. This is a good practice, which should be followed, but we haven't found a good adoption rate by the Vendors developing the software. Even still, authenticity controls do very little without better software development lifecycle controls in place by the vendor. Additionally, the poor record of Certificate Authorities to control certificate validation should be raised.

The cost of putting a process like this in place involves a heavily centralized procurement team and the time to research a large number of vendor practices pertaining to verification. We do not believe the risk reduction justifies this very costly requirement. We propose meeting the FERC directive through R1 and dropping this Requirement altogether.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

The NERC Entity is the customer of the hardware supplier and software supplier, not the designer, manufacturer and developer. As such the Entity can only clearly state what they want the hardware and software to do – at a high level, likely derived from what the vendor said it could do, plus expecting that it will be "bug free". But the Entity should not be expected to have the expertise and tools to "verify the integrity and authenticity of software and firmware" – that is required to be ensured by each step back in the Supply Chain, and that will only happen if each link of the Supply Chain agrees to control their link. CIP-013 is not in a position to impose those controls on the Supply Chain, but only on the end customer. Software and firmware should be expected to be checked for functionality by the Entity.

Likes 0	
Dislikes 0	

Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	

Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes this Requirement is already covered in CIP-007. Having a CIP-013 requirement, that if violated, opens the door to double jeopardy (a finding in CIP-013 would also lead to a finding in CIP-007). There is no need for this Requirement. If there are additional requirements that must be identified, then CIP-013 is not the place for it, CIP-007 is a more appropriate place.	
Likes 0	
Dislikes 0	

Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 3. In addition, we offer the following comments: **Ambiguous Language – "integrity" and "authenticity"**	

The crux of the Requirement is to develop and implement plan(s) that address verification of the “integrity” and “authenticity” of operating systems, firmware, open-source software, and certain patches and upgrades prior to use. Without defining or providing a framework as to what “integrity” and “authenticity” mean, the terms are not measurable for CMEP purposes.

We suggest the Requirement include language that points to established and accepted security frameworks and standards. We offer the following alternative language:

R3. Each Responsible Entity shall manage its Cyber Asset Systems supply chain informed by well-established and accepted cyber security frameworks and standards for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems:

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Concur with EEI’s Position

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

see APPA's comments, with which SVP agrees.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

R3 – line 2 – for clarity purposes NRECA recommends removing “software and firmware.”

Additionally, to the extent possible, NRECA recommends that this requirement should be incorporated into CIP-007 R2 or CIP-010 R1. This is a System Security Management requirement and belongs in the appropriate location. CIP-013-1 and R3.1-R3.4 are all components of the CIP-010 baseline. Placing this topic in a separate standard and requirement creates compliance confusion.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE’s testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity’s capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets, etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.

Likes 0	

Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE's testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets, etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	No
Document Name	

Comment

We don't believe it is reasonable to expect entities to be able to "verify" the integrity and authenticity of software and firmware in all cases. We can attempt to minimize the risk and/or provide reasonable assurance that we have received what was intended. There also needs to be a recognition of the many varied ways that updates and installations of software and firmware might be done most effectively, including the use of automated solutions.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE's testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets, etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC comments on this question and offers the following supplemental comments.

ERCOT recognizes the need for the concepts contained in Requirement R3. However, ERCOT disagrees with the placement of the requirement in a new standard. Since this requirement is applicable to only high and medium impact BES Cyber Systems, it should be placed within CIP-010. The requirement directly impacts the baselines that have been established within CIP-010 R1. The SDT could insert a new part between existing Parts 1.1 and 1.2 in that standard. The new part could use the following language: “For any updates or patches that that deviate from the existing baseline configuration, verify the authenticity and integrity of the update or patch.” As mentioned previously, in developing the CIP Version 5 standards, the SDT performed extensive work to ensure that all requirements related to a particular subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework. Including the requirement in CIP-010 will ensure that a single standard captures all parts of the change process, including inventory (Part 1.1), validation of the code (NEW), authorization of implementation (Part 1.2), update of the inventory (Part 1.3), and testing of the change (Parts 1.4 and 1.5). This approach would give Responsible Entities a complete view of what is required from the start to the end of a change. It also prevents entities from keeping separate inventories to meet the CIP-010 requirement and the CIP-013 requirement.

Additionally, ERCOT requests guidance on how to demonstrate compliance when using automated solutions to obtain the most current patches applicable to their systems. In large environments, these automated solutions are critical to meeting the timing obligations of CIP-007 R2. Inserting the manual step of verifying integrity and authenticity of updates and patches can prevent the use of these solutions that entities have invested in and rely upon for addressing security risks and regulatory obligations. If it is intended that the entity may simply document the source used by these solutions, it would be helpful to put such clarifying language in the requirement.

Additional use cases for the SDT to consider in developing guidance include: (1) how signature and pattern updates are contemplated within the requirement since these are not updates to the operating system, software, or firmware noted, (2) instances when code is packaged and mailed to an entity, (3) software and firmware that are part of a vendor black-box type of appliance solution where the entity has no visibility to the code on the device, and (4) vendors bringing code onsite that the entity is not allowed to review. Any of these cases could present an obstacle to strict compliance with the draft standard language.

As with Requirement R1, this requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. The drafting team should address situations in which vendors will not or cannot provided the levels of service mandated by this requirement. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R3. NERC’s Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company disagrees with the direction the proposed R3 requirement is taking. Given our previous comments under R1 regarding the proper scoping of this new Standard to the “Supply Chain” time horizon, actions proposed to be required under R3 fall outside of that time horizon where the controls are applicable to BES Cyber Systems, which are not yet designated or commissioned as such. Additionally, R3 requires the development of “one or more documented processes” that are in addition to “the plan(s)” required in R1; Southern recommends maintaining the proper scoping of this Standard by moving the components of R3 under R1 to be addressed by the Responsible Entity in “the plan(s).”

If R3 is not consolidated under the R1 requirements for “the plan(s)” to be applicable within the Supply Chain time horizon, then Southern provides the following recommended edits to maintain vital consistency with existing requirements under CIP-010 R1.1. There is firmware in every video card, mouse, hard drive, etc. that is NOT the objective of the requirements in this Standard, but could, without the qualification provided below, be included. The addition under R3.2 also provides vital consistency with CIP-010 R1.1 so we aren’t maintaining different baseline configurations on all of our systems because of slightly different wording in the two Standards.

In this situation where very similar requirements in two different standards create additional administrative burden on entities, the SDT needs to recognize and address the delays that the proposed R3 requirements will have on the existing requirements under CIP-007-6 R2 (Patch Management). The burden of verification of integrity and authenticity of software and firmware in front of applicable requirements for determining availability, applicability, and conducting deployment of security patches within 35 day cycles will make those existing requirements under CIP-007-6 R2 unmanageable and will increase the administrative burden of creating patch mitigation plans as a result of competing Standards.

Modify R3 language as follows:

R3. Each Responsible Entity shall implement one or more documented process(es) that addresses the verification of the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

3.1 Operating System(s) or firmware where no independent operating system exists;

3.2 Commercially available or open-source application software intentionally installed; and

3.3 Patches, updates, and upgrades to 3.1 and 3.2.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment
We agree with this in principal, but this requirement will be extremely difficult to implement and ensure compliance. Currently, numerous vendors do not provide digitally signed patches (Microsoft is notorious for this) or other hashes to verify that a file was not modified. The ability to verify 100% of all software and files will be impossible until vendors are required to implement digital signatures. This can be done via contracts, but it will take time. We highly recommend that the requirement be changed to allow for the fact that software may not be able to be verified and that as long as an entities process checks for this that it is still valid to install with risks.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	

Comment
This appears to be a reasonable approach to meeting the FERC directive.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	

Comment
No Comments

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	

Comment
What other measures or documented evidence should be expected by the Regional Entities when evaluating R3 at audit? An entity could leverage existing CIP-010-2 R1 (3.1-3.3) baseline controls and CIP-007-6 R2 patch management (3.4) controls to support the integrity and authenticity of software and firmware as specified in the CIP-013-1 R3 requirement. However, since the baseline configurations are developed and managed at the BCS level, it is possible that a change to the baseline configuration(s) of a vendor supplied system may not trigger a change to the corresponding baseline configuration for the BCS to which the system(s) is assigned. Therefore, relying on changes to the baseline configuration(s) may not (by itself) be a reliable control to determine if changes were made to a new vendor-supplied system. In such cases, the addition of a simple control (an extra check for new vendor-supplied systems) integrated into an entity's existing CIP-010-2 program would suffice to address the issue.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	

Comment
1. We favor industry accepted methods to address software authenticity such as digital signatures that are consistent with other critical sectors.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
BPA proposes that to truly isolate the production systems from compromised software or firmware more prescriptive language than ‘before being placed in operation’ is required. BPA recommends the SDT develop language to address a supplier that is unwilling or able to support the requirement.

Likes 0	
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

AZPS notes that Requirement R3 requires documented processes for verifying the "integrity and authenticity" of software and firmware before being place into operation and that such language may result in redundant verifications and processes. In particular, software, firmware, etc. are often verified when they are received from the vendor and "incubated" on low risk systems before being pushed to BES Cyber Systems. To avoid the need to "re-verify" these updates after incubation, but prior to placement in production on BES Cyber Systems, AZPS requests the following change to Requirement R3,

'…verifying the integrity and authenticity of the following software and firmware ***being placed in operation on high and medium impact BES Cyber Systems***, **when received**'. Additionally, Requirement R3 addresses the verification of integrity and authenticity of software and firmware; however, it does not address the likelihood of a vendor's inability or unwillingness to comply. AZPS requests clarification of whether an inability to verify would be considered a failure to implement the process if verification is not possible due to vendor inability or unwillingness.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG agrees with the intent of this requirement, but has the following questions/recommendations below:

- The way this requirement is written, it may not be possible to perform a technical verification of software integrity and authenticity. How does the standard drafting team expect registered entities to address this if it cannot be done in a technical manner?
- Requirements R1 and R2 do not require the registered entity to go back and revise previous contracts. In order to comply with this requirement, R3, changes to past contracts / vendor service agreements may be required. Alignment is needed between R1, R2, and R3.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	Yes
Document Name	

Comment

We recommend the SDT address virtualization and CIP Exceptional Circumstance with respect to this requirement aligned with project 2016-02.

Also please see our earlier comments with regards to redundancy between R3 and R1.2.5.

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5

Answer	
Document Name	

Comment

Suggest striking the word “associated” from the phrase “software, firmware, and associated patches”.

Basin Electric recommends adding language to address potential Technical Feasibility Exception (TFE) such as:

R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware**, where technically feasible,** before being placed in operation on high and medium impact BES Cyber Systems:

In R3.2, “Firmware” is already included in R3 which is redundant in R3.2. Basin Electric recommends R3 be written as a general Requirement with specifics in the sub Requirements.

There are a lot of parallels between these requirements and the requirements already required in CIP-007 R2 patch management controls. Basin Electric would rather see these obligations integrated into CIP-007.

The rationale explains the obligation for this requirement starts in the operate/maintain phase of the life cycle, but the timing/life cycle language is not included in requirement. Basin Electric suggests modifying the requirement to include clarification of when the obligation starts. Perhaps add language to the front of R3 such as: “For Cyber Assets in production…”

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	
Document Name	

Comment

N/A

Likes 0	
Dislikes 0	
Response	

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

As written, R4 is more appropriately addressed in other existing standards, CIP-004 for authorization, CIP-005 for remote access, CIP-007 for logging, and CIP-008 for response. Furthermore, it confuses the expectation of all these standards from an audit perspective by duplicating or undermining existing requirements. Authorization for interactive remote access is already covered in CIP-004 R4. Logging and monitoring of access to an Intermediate System or BES Cyber Asset is already covered in CIP-007 R4. If an entity requires separate evidence for those standards and CIP-013 R4, this could present a double jeopardy situation for compliance where an entity can be audited and penalized twice for similar requirements if a Regional Entity does not find their methods of compliance satisfactory.

Controlling remote access, including vendor remote access, is already addressed in CIP-005 R1 and R2 so CIP-013 R4 will overlap with those existing requirements. CenterPoint Energy recommends changing “system-to-system remote access with a vendor” to “vendor initiated system-to-system remote access” and modifying existing requirements if necessary, rather than including the requirements in CIP-013.

R4.3 is part of an entity’s incident response plan, and should be in CIP-008.

R4.2, R4.3 sub-requirements both need clauses for per Cyber Asset capability or technical feasibility exceptions.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

2) Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

3) The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

4) Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

5) Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6) The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

Likes 0	
Dislikes 0	
Response	

Richard Vine - California ISO - 2

Answer	No
Document Name	
Comment	

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	

Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move,

such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

SCE&G agrees with EEI in its assessment regarding R4:

"The use of "activity" in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as "escorted cyber access." In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions… We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3."

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

1. R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.
2. Recommend that this Rationale needs to be updated from "machine-to-machine" to "system-to-system" for consistency
3. The first sentence of R2 is broader than the second sentence. The first sentence is "Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems." The second sentence is "The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):" Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.
4. Request guidance. "Vendor-Initiated" could be considered a single word and not associated with the proposed definition of "vendor".

5. Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6. The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

7. Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

8. R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

9. For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3.

10. This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs.

11. Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2.

12. SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG suggests that R4, Section 4.1, Section 4.2, Section 4.3 language be moved to CIP-005. Since this is interactive remote session specific, NRG recommends moving all of these requirements into CIP-005 because of the implied real-time monitoring and logging requirements. Even though there are monitoring requirements in CIP-007, the monitoring requirements of CIP-007 are more forensic in nature. Various vendors and entities will likely want to implement individualized solutions to manage this requirement which will become administratively burdensome to the industry. These varied solutions can also present more ports being open (a reliability /security risk) to High and Medium BES Cyber Systems which could lessen reliability. NRG recommends that scope of this requirement should be for High and Medium with ERC BCS.

NRG requests that the SDT provide clarity that “system-to-system” is equivalent to “machine-machine” and what does it mean (i.e. application interface vs. laptop/server level). NRG recommends reference to the OSI layers. The R4 rationale appears to be inconsistent with the FERC directive regarding “machine to machine”. NRG requests clarification of whether the rationale / intent of “system-to-system” is meaning that a direct machine to machine interface is needed or that it needs to go through an intermediate or third host (jump host). NRG requests that the term “vendor” be defined to clarify intent of meaning a company or an individual (in the context of interactive remote access).

In the implementation plan for this standard, NRG recommends a staggered implementation plan for R1, R2 & , R5 being 15 calendar months. However, NRG recommends a 24-month implementation plan for R3 & R4would be needed for Registered Entities to manage this process on all impacted systems due to the need to re-negotiate processes with vendors (individualized solutions).	
Likes 0	
Dislikes 0	
Response	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
SCE&G agrees with EEI in its assessment regarding R4: *"The use of "activity" in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as "escorted cyber access." In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions… We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3."*	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	
• Interactive Remote Access controls are defined in CIP-005 and in CIP-007. These requirements are duplicative and create the possibility of double-jeopardy for non-compliance. In addition, CIP-004-6 R4 Part 4.1.1 specifically addresses electronic access. Dominion is of the opinion that CIP-013-1 should concentrate on supply chain obligations for system-to-system communications which isn't addressed under the existing CIP standards. Operational requirements, such as the proposed R3, should be added to the appropriate CIP standard. • Dominion recommends removal of Part 4.2. Complying with the logging requirement could degrade system performance to the point where the BES reliability would be negatively impacted. Additionally, the monitoring requirement further degrades the performance, and may not be technically feasible. • If Part 4.2 is retained, the requirements should state the minimum criteria for logging and monitoring unauthorized access, as currently outlined in CIP-007-6 Part 4.1.	

- The terms “access” and “activity” as used in the proposed CIP-013-1 need to be defined.
- Read only access should be excluded from the final requirement based on definition of Interactive Remote Access.
- Dominion recommends the removal of Part 4.3 Disabling or otherwise responding to unauthorized activity during remote access sessions seems to imply an on-going monitoring of active connections to a degree that’s not technically feasible.
- If Part 4.3 is retained, we recommend that the minimum criteria for logging and monitoring be limited to disabling what has been detected. Dominion recommend the following language to achieve this goal:

4.3: Disabling or otherwise responding to detected, logged, and monitored unauthorized activity during remote access sessions.

- Dominion recommends creating a definition “system-to-system remote access” in the NERC glossary. Using a broad undefined term can lead to inconsistent results.

Likes 0	
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

Specific operational cyber security controls are best addressed as revisions to CIP-002 through -011.

Refer to EEI comments on R4 which point out overlaps to existing requirements in CIP-004, -005 and -008.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives’ deadlines, NERC and industry should reprioritize SDT teams’ work and resources.

We further point out the FERC Order 829 has directed revisions to remote access (for vendors) by Sept. 2017 which is before FERC’s Order 822 P64 directive to NERC for a CIP version 5 remote access controls effectiveness study is even due. The remote access controls effectiveness study is not due till June 30, 2017.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move,

such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

The proposed Requirement creates significant overlap with existing CIP Requirements. Requirement R4, as well as Requirements R3 and R5, should be modified so that CIP-013 only addresses those aspects of software integrity and authenticity (R3), remote access (R4), and authenticity and remote access for low impact BES Cyber Systems (R5) not covered by other Standards. Exelon understands that the timeframe dictated by FERC in Order No. 829 does not allow for revisions by this SDT to the relevant Standards that address these topics. However, overlap between the Standards should be avoided as much as possible to avoid double jeopardy concerns in the event of potential non-compliance with CIP-013 R3, R4, and R5.

For example, Exelon's review of the draft CIP-013-1 Standard indicates the following areas of overlap:

• CIP-013-1 R3.1 through R3.4 require authentication of operating systems, firmware, software, and patches. However, the configuration change management requirements under CIP-010-2 R1 already require that the configuration of operating systems, firmware, and software be carefully tracked such that counterfeit operating systems, firmware, software, and patches would be identified (e.g. a software difference would be identified as a change from the existing baseline configuration) and would be evaluated.

• CIP-013-1 R3.4 requires authentication of patches, updates, and upgrades, but CIP-007-6 R2.1 already imposes a patch management process for tracking, evaluating, and installing cyber security patches, including the identification of patching sources. Part of the identification of patching sources under CIP-007-6 is the verification that those sources are authentic as CIP-013-1 R3.4 would appear to require.

• CIP-013-1 R4.1 requires authorization of remote access to certain BES Cyber Systems by the vendor. CIP-004-5 R4.1.1 already contains a process for authorizing electronic access to these assets by all personnel, including vendors.

• CIP-013-1 R4.2 requires logging and monitoring or remote access sessions. CIP-007-6 R4.1 already requires logging of all access and CIP-007-6 R4.2 requires alerting for any malicious code as well as any "security ecent that the Responsible Entity determines necessitates an alert."

• CIP-013-1 R4.3 also requires responding to detected unauthorized activity, and because unauthorized activity on a BES Cyber System would constitute a "Cyber Security Incident," CIP-008-5 already requires a response to such incidents.

• CIP-013-1 R5 requires a process for controlling vendor remote access to low impact BES Cyber Systems. This overlaps with CIP-003-6 Attachment 1 Section 3 which already requires electronic access controls for low impact BES Cyber Systems the limit access to necessary access.

The draft CIP-013-1 requirements should be modified so that overlaps are removed and that CIP-013-1 only addresses vendor issues not covered within existing Standards. To the extent the SDT believes there is no overlap between CIP-013 and the existing CIP Standards, the SDT should explain in each instance where the CIP-013 Requirement ends and the other CIP Requirement begins. In the absence of such guidance, a Compliance Monitoring and Enforcement Process could conclude that a particular instance of non-compliance with CIP-013 is also a simultaneous violation of another Reliability Standard, doubling the available penalty range. For example, draft CIP-013-1 R4 requires the Responsible Entity to authorize remote access by vendor personnel. The current CIP-004-6 R4.1.1 also requires authorization of vendor personnel to have electronic access. Therefore noncompliance with CIP-013-1 R4 would appear to, per se, constitute noncompliance with CIP-004-6 R4.1.1. Such double jeopardy serves no apparent

reliability purpose. If the current CIP-013-1 R4 language is adopted as-is, the SDT should explain how its requirements differ from those under CIP-004-6 R4.1.1.

Finally, Exelon suggests that R4.3 may be difficult to accomplish in all cases and is overly prescriptive and thus should be removed from CIP-013. Order No. 829, P.52 references the Ukraine event and 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." There are alternate methods to address this threat. First, two factor identification methods can be used to mitigate the risk of stolen credentials. Second, the use of WebEx or Skype sessions or active control of vendor access (i.e. opening a port for access only when needed) can be used to address emergent issues and reduce the need for remote persistent sessions.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining "unauthorized activity" if that is not changed to "unauthorized access".

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We suggest that Requirement R4 Section 4.1 language be moved to the CIP-004 Standard. The group feels that CIP-004 Part 4.1 already handles access controls in that particular Cyber Standard. Additionally, we feel that a potential conflict may exist between CIP-013 Requirement R4 and CIP-004 Requirement R4 if this Requirement stays in its current position.

As for Section 4.2 language being moved to the CIP-007 Standard, our group feels that the CIP-007 Standard already addresses logging.

Finally, we suggest moving Section 4.3 Language to the CIP-005 Standard because, we feel that the CIP-005 Standard already addresses interactive access to BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Authorization of remote access to BES Cyber Systems (Part 4.1) is already addressed by CIP-004-6 R4 for user-initiated remote access and implicitly by CIP-005-5 R1 Part 1.3 (“Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”) for machine-to-machine access. It should be deleted.

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment

See Comments on Requirement R4 in attached file.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

After moving to CIP-005, R4.2 should be revised to say: “Capability to detect unauthorized activity; and”

R4.3 should add the word “detected” before the term “unauthorized activity.”

For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3.

This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs.

Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2.

Suggest that this Rationale needs to be updated from “machine-to-machine” to “system-to-system.”

SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5

Answer	No
Document Name	

Comment

R4 appears to be in parallel to requirements that already exist in CIP-004, CIP-005, CIP-007 and CIP-008. Basin Electric would prefer the requirements be integrated with the existing standards.

Basin Electric believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, Part 4.3 should be taken care of by complying with CIP-005-5 Part 1.3 which requires inbound and outbound access permissions which prevent unauthorized activity.

R4, Part 4.3 “otherwise responding” should be taken care of by complying with CIP-008-5 R2.

In the context of R1–R3, the term “vendor” appears to apply to a company as stated in the rationale section. In context of R4, the same term “vendor” now appears to mean individual personnel who represent a company. Clarity is needed on who this requirement actually applies to.

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1

Answer	No
Document Name	

Comment

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	

Comment

- The scope of CIP-013-1 R4 appears to overlap with parts of CIP-005-5R1.3, R1.5, R2.1 - 2.3; and CIP-007 R4.1, R4.2, R5.7. (Both of the CIP-007 and CIP-005 requirements apply to High and Medium BCS and associated EACMS, PACs, and PCAs). However, the logging and monitoring requirements in CIP-007-6 R4.1, 4.2 specifically cite “per Cyber Asset capability” and “after-the-fact investigations.”
    - Additionally, the CIP-013 requirement indicates “Disabling or otherwise responding to unauthorized activity during remote access sessions.” Not all technologies would have the capability of real-time cyber asset level user activity monitoring, needed to detect activity and disable sessions.
    - CIP-013 R4 does not consider the variability of cyber asset capability. Not all technologies can support cyber asset level logging.
- A definition of “unauthorized activity” is needed. Note: existing processes in CIP-004 establish authorized activity for vendors, contractors, and employees, including: training, PRA, and access management. Security controls in CIP-005 and CIP-007 enforce the limits of those authorizations. Vendors who are granted specific access rights to remotely access systems are, by definition, authorized to perform certain functions. Jump-hosts, firewalls, user accounts, and application privileges already limit activity to permitted activity.
- “Machine-to-machine vendor remote access” should be defined, or the formal definition of “Interactive Remote Access” should be modified to include machine access.
- “Monitoring” should be defined. Suggested clarification is that monitoring includes information regarding the startup and termination of the connection, but does not include the capturing of user activity during the session.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment

SRP requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. SRP requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. SRP requests changing the language to “upon detected unauthorized activity”.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	

Comment

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment

We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	

Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

CIP-013 R4.1 is duplicative of CIP-004 R4.3 as all persons already require authorization of electronic access to the systems in scope of this requirement. As entities will have to follow duplicate requirements in two different standards, CIP-004 and CIP-013, there is an increased likelihood of a violation.

CIP-013 R4.2, Logging, monitoring, and alerting is already covered in CIP-007 R4.1 and R4.2. An additional requirement part in CIP-007 R4 would be the most effective place to meet this FERC expectation. As entities will have to follow duplicate requirements in two different standards, CIP-007 and CIP-013, there is an increased likelihood of a violation.

CIP-013 R4.3 would be handled best as a component of CIP-007 R4 for detected inappropriate access. Alerting is already required by CIP-007 R4.2 and a simple additional step (requirement part) would require a response to the alert. The guidelines and technical basis should discuss use of intrusion prevention systems to meet this requirement without requiring significant additional compliance evidence.

Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

R4 creates confusion and possible double jeopardy with other standards. Recommend modifying modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 address the FERC order No. 829.

Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to detected unauthorized activity.“

For R4.3, the “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Suggest changing to “detected unauthorized activity”.

Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. AE requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. AE requests changing the language to “upon detected unauthorized activity”.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	
PRPA requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access. Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. PRPA requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. PRPA requests changing the language to “upon detected unauthorized activity”.	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.	

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AECI supports the following comments from the MRO NSRF:

“The NSRF believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, P4.3 should be taken care of by complying with CIP-005-5. Part 1.3 of CIP-005-5 requires inbound and outbound access permissions which prevent unauthorized activity.”

Furthermore, AECI contends that the SDT should remove this requirement and address vendor remote access in the implementation of the supply chain risk management plan(s) as detailed in the requirement concepts proposed by AECI in Question 1. This concept will allow Responsible Entities to address the issue contractually with applicable vendors.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC comments.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	No
Document Name	

Comment

We request confirmation that vendor access does not include onsite staff augmentation contract resources. Clarification is also requested on whether "system to system" access applies to access that is "one-way" where the remote end conducts only monitoring activity and no control is possible. Can the procedure for access make distinctions for each method of monitoring each type of access, Interactive Remote, system to system with control and system to system for monitoring only? Finally, the term "unauthorized activity" is unclear. We recommend using the term "unauthorized access".

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	

Comment

The rationale section in Requirement R4 speaks to “machine-to-machine vendor remote access” while the actual requirement speaks to “system-to-system remote access with a vendor”. ReliabilityFirst recommends the SDT use consistent language so that there is no confusion on terminology or definitions.

Requirement R4 mentions high and medium BES Cyber Systems, but does not include their associated Electronic Access Control and Monitoring Systems (EACMs), Physical Access Controls(PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following modifications for consideration:

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems [and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets]. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy recommends that the drafting team consider creating a definition for the terms “vendor” and “unauthorized activity”. Without clear expectations as to what is considered unauthorized activity, and further technical guidance on how to detect this type of activity, the Responsible Entity will not be able to determine what to look for to comply with R4.2, and will not know when to disable this activity to comply with R4.3.

We request further clarification from the drafting team on what is meant by “*vendor-initiated Interactive Remote Access”.* Does this refer to access that originates from a non-Responsible Entity system? Also, does “*remote access*” apply in the instance where a non-Responsible Entity party accesses a BES Cyber System remotely to the ESP, but is originating on a network inside of the Responsible Entity’s infrastructure? Should the requirement language be revised to better categorize remote access as “external” remote access originating from a location that is not a Responsible Entity’s facility or location?

Likes 0	
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	No
Document Name	

Comment

Please consider consolidation of R4 requirements into CIP-005 instead of a separate requirement to assist REs who may utilized shared processes and systems for providing Interactive Remote Access, regardless of the origin of the remote access.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

This risk should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-005 R2, CIP-004 R4, and CIP-007 R4.

IID feels that there should be an exclusion comparable to a CIP Exceptional Circumstance (or Technical Feasibility Exception) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

Likes 0	
Dislikes 0	

Response

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3

Answer	No
Document Name	

Comment

This seems not to be a supply-chain issue. It would seem that NERC's intent is to wrap-up order 829 into a single standard instead of modifying the existing standards (CIP-005 Requirement 2), where necessary, to address these weaknesses.

There should *most definitely* be a feasibility exception with respect to 4.2 and 4.3.

What does 'during remote access sessions' mean in 4.3? If the session is active, it would be prudent to expect immediate termination of the connection as the Guidance suggests – responding in a timely manner. Termination during a remote access session could imply a normal, or 'timed' termination of the connection, long after an intended response to unauthorized activity would ordinarily occur.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	No
Document Name	

Comment

R4 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R1 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R4 should be rewritten to be only applicable to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	No
Document Name	

Comment

R1.2.6 is duplicative of R4. These requirements should be made consistent, or one of them should be deleted.

Much of R4 is already covered by CIP-005 (R1 and R2), CIP-007 (R4) and CIP-008. Requirements for a single topic should be consolidated within a single standard.

Likes 0	
Dislikes 0	

Response

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, P4.3 should be taken care of by complying with CIP-005-5. Part 1.3 of CIP-005-5 requires inbound and outbound access permissions which prevent unauthorized activity.

Remove "disable or other responding" and replace with "Response". Leave the options for response with the Register Entity.

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company strongly disagrees with the direction the proposed R4 requirement is taking, while recognizing the time constraints placed on the SDT to file a new or modified Standard addressing Supply Chain risks. As currently drafted, R4 carries significant overlap and repetition with existing CIP Standards, specifically with CIP-004-6 R4, CIP-005-5 R1, CIP-007-6 R4, and CIP-008-5 R2. "Authorization of remote access" should be deleted because in no way can you circumvent CIP-004-6 R4.1 requiring authorization of remote access to a high or medium impact BES Cyber System and there is no need to replicate that requirement again in this Standard. Additionally, CIP-005 R1.3 requires explicit access permissions and documented business justifications for all 'system-to-system' access, including vendor-initiated access. With respect to "logging and monitoring", and the detection of "unauthorized activity", we have serious concerns over the proposed language and provide that CIP-005-5 R1.5 already requires the detection of inbound and outbound malicious communications, CIP-007-6 R4 already requires the logging and controlling of access at each ESP boundary and to BES Cyber Systems, and CIP-008-5 R2 already requires response to detected Cyber Security Incidents, which includes unauthorized activity during a vendor remote access session. As drafted, a failure to comply with R4 could place a Responsible Entity in possible double jeopardy with those other requirements. Additionally, as written, R4 creates a scope expansion of the existing CIP-005-5 R1.5 currently applicable to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers to now ropes in all Medium Impact BES Cyber Systems – leaving entities (and auditors) to determine "which Standard wins?"

Based on those concerns, Southern Company recommends the complete removal of R4 from the Standard, and where additional controls not already covered in an existing Standard are directed in the FERC Order, those controls should be covered under "the plan(s)" under R1 in a similar manner as the proposed edits provided under R1.

If R4 is not removed in this manner, we provide the below edits for consideration with the following comments. In addition to the justified removal of "authorization of remote access", logging and controlling are achievable concepts due to their requirement under existing Standards and therefore should not be required again here in this Standard and removed. This leaves "methods to disable remote access sessions", which we propose moving under the main R4 for the applicable scenarios. Again, detecting and responding to "unauthorized activity" is already required under existing Standards, and should be removed from R4. If not removed, the SDT must address the discrepancy between the scope collision between the draft R4 and CIP-005-5 R1.5.

Additionally, if there is an expectation beyond the use of IDS/IPS for "detecting unauthorized activity", then we would argue that it is nearly impossible for an entity to look at a stream of 1's and 0's flowing by at a several megabits per second and determine whether there is "unauthorized activity" or not in that stream. With the difficulty in determining "unauthorized activity" in a stream of bits flying by, we respectfully recommend striking this and request the SDT to consider focusing the controls in this requirement specifically to having methods to rapidly "disable remote access" to prevent remote control of entity assets.

Modify R4 language as follows:

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall address methods to disable remote access sessions for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s). [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT supports the IRC comments and offers the following supplemental comments.

Requirement R4 is duplicative of existing requirements in CIP-004, CIP-005, CIP-007, and CIP-008. The drafting team should consider modifications to these existing standards rather than creating new requirements in a new standard. By placing these requirements in a stand-alone Standard, there is a possibility that entities may not make necessary connections to the prerequisites of some requirements (e.g., CIP-004 R2, R3) and downstream obligations of other requirements (e.g., CIP-008). ERCOT offers the following suggestions for realignment:

Requirements for electronic access authorization of vendors, including Interactive Remote Access, are addressed within CIP-004 R4, which also addresses the proper vetting and training of said vendors. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper pre-authorization requirements.

Requirements for Interactive Remote Access are already addressed within CIP-005 R2. Vendor-initiated remote access is just one example of Interactive Remote Access. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper configuration of remote access (e.g. multi-factor authentication, encryption, Intermediate System).

Requirements for system-to-system communications are already addressed within CIP-005 R1. This requirement could be added to CIP-005 R1 or as an addition to R2. The heading for Table 2 within CIP-005 can be modified to “Remote Access” in support of this. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper network controls for the system-to-system communication (e.g. ESPs, EAPs, etc.).

Requirements for logging and monitoring of access activity are addressed in CIP-007 R4. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify the logging specifications that differ from CIP-007 R4.

Requirements for response to unauthorized activity are already addressed within CIP-008. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify integration with CIP-008.

There are also several instances in the standard where language needs to be clarified. The drafting team should state whether system-to-system remote access includes “phone home” capabilities that are used for reporting of licensing, system health, and system problems. Requirement R4.1 should be clarified to specify whether it is addressing authorization of each remote access session or remote access to the vendor in whole. The drafting team should consider whether this requirement is consistent with current requirements in CIP-004 R4. The drafting team also needs to address authorization of software companies that use a “follow-the-sun” support model. Follow-the-sun is a type of global support where issues are passed around daily between work sites that are many time zones apart. Such a support increases responsiveness.

As noted with other requirements in the draft CIP-013 standard, the drafting team should address situations in which vendors will not or cannot provide the levels of service mandated by this requirement. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling to agree. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R4. NERC’s Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Likes 0	
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	No
Document Name	

Comment

We are in general agreement with EEI comments on this requirement.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Scott Downey - Peak Reliability - 1

Answer	No
Document Name	

Comment

Access into the ESP is controlled for vendors the same as FTEs. That process is already outlined in other CIP requirements. If this is meant to be an alternative avenue of access outside the rest of the standards that is not clear.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

The standard should not create additional requirements for which entities are already being audited against. This creates confusion and risks the entity to being in double jeopardy for the same activity. NRECA recommends revising R4 to address the following:

R4, Part 4.1 is already covered under CIP-004-6 R4, Part 4.1

R4, Part 4.2 is already covered under CIP-007-6 R4, Part 4.1

R4, P4.3 is already covered under with CIP-005-5

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

- See APPA's comments, with which SVP agrees.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
We have questions and concerns about how R4 would be applied. Please see the associated comments in Question 9.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
This Requirement is duplicative of CIP-005-5.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	

Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 4.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes identifying and logging unauthorized access is already covered. In CIP-005. Furthermore, SunPower believes that 4.3, disabling the threat of unauthorized access to BES Cyber Systems should be addressed through a revision to CIP-007, where controls for external access are covered.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No

Document Name	
Comment	
The NERC CIP Cyber Security Standards already have one of the most specific remote access security standard through CIP-005. Additional specifications to remote access should not be placed in a supply chain cyber security risk management Standard.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

2) Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

3) The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

4) Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

5) Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6) The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3.

This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs.

Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2.

SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No

Document Name	

Comment

Control of Interactive Remote Access to High and Medium Impact BES Cyber Systems is already required by CIP-005-5, Requirement R2. To that end, including that aspect in this Requirement is duplicative to some extent. Similarly, it could be argued that authorization of remote access is covered by CIP-004-6, Requirement R4, and logging of access is required by CIP-007-6, Requirement R4. The Standards Drafting Team should either incorporate the few remaining elements into the existing Requirements in the other CIP Standards, or rewrite this Requirement to only include the additional expectations not covered elsewhere.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC disagrees with the proposed requirement. CIP-013-1 R4 requires actions to be taken by the Responsible Entity that are outside of the supply chain context. FERC Order 829 specifically stated in paragraph 45 that the plan should address the security objectives in "the context of addressing supply chain management risks." NIST 800-53 provides a definition of supply chain that is as follows: "Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer." FERC Order 829 acknowledges this definition in paragraph 32, footnote 61. However, the SDT has chosen to identify controls in R4 that are executed only as part of the day-to-day management of BES Cyber Systems and introduce double jeopardy with existing CIP Reliability Standards.

R4 as written contains three parts to each be implemented for "(i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)."

4.1: Authorization of remote access. Electronic access to high and medium impact BES Cyber Systems, whether local or remote, and regardless of whether the individual is a vendor, is already required by CIP-004-6 R4, Part 4.1. System to system remote access must be explicitly permitted through the ESP along with documented justification according to CIP-005-5 R1, Part 1.3.

4.2: Logging and monitoring of remote access sessions: CIP-005-5 R1, Part 1.5 requires methods for detecting malicious communications for high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers. CIP-007-6 R4, Part 4.1 requires logging of successful and failed access attempts. The applicable systems for CIP-007-6 R4, Part 4.1 includes EACMSs associated with medium and high impact BES Cyber Systems, effectively including logging that occurs at the perimeter of the ESP as well as access to the BES Cyber Systems directly. CIP-007-6 R4 additional requires monitoring of the logs.

4.3: Disabling or responding to unauthorized activity: CIP-008-5 R2 requires that entities respond to unauthorized activity according to their defined incident response plans. As a Cyber Security Incident includes any incident that "compromises, or was an attempt to compromise, the ESP…" or "disrupts, or was an attempt to disrupt, the operation of a BES Cyber System," response to any unauthorized activity (whether local or remote, physical or electronic) is already required by CIP-008-5 R2.

That said, there are gaps remaining between the existing CIP standards and the directive as specified by FERC Order 829.

As such, all controls required by CIP-013-1 R4 already exist in other CIP Reliability Standards, effectively making any non-compliance with R4 a case of double jeopardy with either CIP-004-6 R4, CIP-005-5 R1, CIP-007-6 R4, or CIP-008-5 R2, depending on the facts and circumstances of the specific compliance issue. While CIP-013-1 R4 suggests the implementation of technical security controls, it is unclear what additional controls would be implemented that are not already required by the existing CIP Standards. CIP-013-1 R4 only provides for additional paperwork, administrative burden, and double jeopardy compliance risk. As such, the standard drafting team should not create additional requirements for which entities are already being audited against and it should be removed.

That said, we do believe that addressing remote access in the supply chain context (not in the day-to-day operations context) could provide supply chain security risk management benefits. Unfortunately, the SDT has not constructed its requirement as such. Consistent with our response to question 1, we recommend that the SDT consider a plan based approach to addressing security risks in the context of the supply chain.

R4 is written in a manner that implies the Responsible Entity shall implement a separate documented process in addition to the plan specified in R1. Paragraph 45 of Order No. 829, clearly specifies this objective of vendor remote access should be applied to "The Plan" identified in the core directive in the context of addressing supply chain management risks.

(P. 45) The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

GTC recommends the SDT remove this requirement and include a security objective for vendor remote access in "The Plan" specified in R1 to align with the FERC Order. See GTC's comment for Question #1.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. We recommend that the SDT consider changing “activity” to “access” in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard “must address responsible entities’ logging and controlling all third-party (i.e., vendor) initiated remote access sessions.” (Order No. 829, P51) The security objective is to address “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.” (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated “Charles Angels” style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a “how” to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor’s ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the “monitoring” language to “control” and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it’s unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No

Document Name	
Comment	

The IRC and SWG request that the SDT consider moving this requirement to existing CIP Standard to prevent overlap, conflict, or omission of existing requirements.

The SDT should address whether system-to-system access is when vendor-initiated. Lack of clarity there will impact automated updates from vendors that are time-sensitive, as well as outbound connections to vendors for health checks, licensing, and other system information.

Likes 0	
Dislikes 0	
Response	

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	
Comment	

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. We recommend that the SDT consider changing “activity” to “access” in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard “must address responsible entities’ logging and controlling all third-party (i.e., vendor) initiated remote access sessions.” (Order No. 829, P51) The security objective is to address “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." (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated "Charles Angels" style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a "how" to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor's ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the "monitoring" language to "control" and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it's unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

This requirement is duplicative of existing requirements within CIP standards.

Authorization of access is covered in CIP-004-6 R4.1. The language in this CIP-004-6 R4.1 does not exclude vendors.

The rationale for CIP-007-6 R4 explicitly states that security event monitoring's purpose is to detect unauthorized activity.

A detection of unauthorized activity would be investigated as a potential Cyber Security Incident and appropriate action would be taken from there.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language. These operations requirements are covered in other CIP standards.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. We recommend that the SDT consider changing “activity” to “access” in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard “must address responsible entities’ logging and controlling all third-party (i.e., vendor) initiated remote access sessions.” (Order No. 829, P51) The security objective is to address “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." (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated "Charlie's Angels" style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a "how" to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor's ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the "monitoring" language to "control" and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it's unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of

Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	

SMUD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. SMUD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. SMUD requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	
Response	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	

The NYPA Comments	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx
Comment	

The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.

Seattle City Light requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Seattle City Light requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Seattle City Light requests changing the language to "upon detected unauthorized activity".

Furthermore, because it may not be technically feasible to remotely disable a vendor from equipment provided by that vendor (which the entity purchased from them, and may be dependent upon the vendor for maintenance), Seattle City Light requests the inclusion of a Technical Feasibility Exception (TFE) for R4. Seattle City Light suggests the following language: "WHERE TECHNICALLY FEASIBLE, each responsible entity shall implement one or more documented process(es) for controlling vendor remote access to…" (emphasis added).

Likes 0	
Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2

Answer	No
Document Name	

Comment

The IESO request that the SDT consider moving this requirement to existing CIP Standard to prevent overlap, conflict, or omission of existing requirements.

The SDT should address whether system-to-system access is when vendor-initiated. Lack of clarity there will impact automated updates from vendors that are time-sensitive, as well as outbound connections to vendors for health checks, licensing, and other system information.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	No
Document Name	

Comment

Colorado Springs Utilities (CSU) requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. CSU requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CSU requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry

Answer	No
Document Name	

Comment

See EEI comments

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend modifying modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 address the FERC order No. 829.

2) For R4.3, the “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Suggest changing to “detected unauthorized activity”.

3) Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA believes the scope should be limited to High and Medium BES cyber systems with ERC or dialup. All requirements for Low impact systems should be addressed in CIP-003.

BPA suggests modification of existing CIP standards to address gaps:

Remote access CIP-013 R4, P4.1 is addressed in CIP-004-6 R4, Part 4.1

Logging and monitoring CIP-013 R4, P4.2 is addressed in CIP-007-6 R4, P4.1

Remote access sessions CIP-013 R4, P4.3 is addressed in CIP-005 R2

Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	

This requirement is duplicative of existing requirements within CIP standards.

Authorization of access is covered in CIP-004-6 R4.1. The language in this CIP-004-6 R4.1 does not exclude vendors.

The rationale for CIP-007-6 R4 explicitly states that security event monitoring's purpose is to detect unauthorized activity.

A detection of unauthorized activity would be investigated as a potential Cyber Security Incident and appropriate action would be taken from there.

Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Santee Cooper requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Santee Cooper requests changing the language to "upon detected unauthorized activity".

Likes 0	
Dislikes 0	
Response	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
Rationale for Requirement R4: The rationale language for R4 states, “The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51).” R1, R2, and the Rationale for Requirement R3 and R4 do not specify the impact classifications (High, Medium and Low) when referencing the BES Cyber System. R3 and R4 specifically state the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems (R3)” or “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems (R4).” IPC would like to know if the inconsistent impact classification references were intended or were an oversight by the SDT? **R4** IPC does not believe CIP-013-1 is an appropriate standard to address R4.1, R4.2 and R4.3. IPC believes R4.1 belongs in CIP-004-6, as R4.1 is related to authorization and R4.2 and R4.3 belongs in CIP-005-6 as R4.2 and R4.2 are related to remote access. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-004-6 addresses access management and CIP-005-6 addresses remote access. **M4** Some of the measure language for R4 states, “hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.“ R1, R2, and the Rationale for Requirement R3, R4, and M4 do not specify the impact classifications (High, Medium and Low) when referencing the BES Cyber System. R3 and R4 specifically states the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems (R3)” or “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems (R4).” IPC would like to know if the inconsistent impact classification references were intended or were an oversight by the SDT?

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016. Reclamation recommends that Requirement R4 be deleted. There would be no need for Requirement R4 if all aspects of the supply chain risk management plan(s) are to be addressed in Requirement R1 and its sub-requirements.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	
1. As mentioned above, the standard drafting team should not create additional requirements for which entities are already being audited against. This creates confusion and risks the entity to being in double jeopardy for the same activity. R4, Part 4.1 is covered under CIP-004-6 R4, Part 4.1 R4, Part 4.2 is covered under CIP-007-6 R4, Part 4.1 R4, P4.3 is covered under with CIP-005-5. Part 1.3 of CIP-005-5	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	No
Document Name	

Comment

Requirement R4:

ATC agrees with the value provided through the implementation of controls to address logging and controlling third-party initiated remote access; however, ATC has voted “No” to the proposed language developed CIP-013-1 Requirement R4 because existing Reliability Standards accomplish this objective rendering the need for this requirement in CIP-013-1 moot. In its redundancy, it is at odds with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

Requirement R4 Sub Requirement 4.1 – 4.3:

CIP-013-1 R4 is simultaneously duplicative and additive to the language and/or intent of several existing approved and effective CIP Cyber Security Reliability Standards and is therefore providing no additional security or reliability value and creating a condition of double jeopardy for Registered Entities where a violation of CIP-013-1 R4 would constitute a violation of another CIP Standard and requirement.

CIP-004-6 R4 and R5 address access management and revocation for individuals having cyber access to specified high and/or medium impact-rated BES Cyber Systems and associated Cyber Assets. The existing enforceable CIP-004-6 standard is silent to the capacity with which a given individual is engaged with a Registered Entity, and therefore in its silence it addresses employees, contractors, interns, apprentices, or even vendors etc. These access requirements within CIP-004-6 are more prescriptive than what is proposed for CIP-013-1 therefore providing no additional security or reliability value and ultimately rendering CIP-013-1 R4.1 superfluous and unnecessary.

CIP-005-5 R1 Parts 1.1 – 1.4 addresses CIP-013-1 R4(i), R4.1, ultimately rendering CIP-013-1 R4(i), R4.1 superfluous and unnecessary in that:

- CIP-005-5 R1 Parts 1.3 mandates authorization for system-to-system remote access through the requirement for inbound and outbound access permissions through an identified Electronic Access Point protecting high and/or medium impact-rated BES Cyber Systems,
  - where those BES Cyber Systems must already be protected as a function of being inside an identified Electronic Security Perimeter pursuant to CIP-005-5 Requirement R1 Part 1.1, and
  - where all External Routable Connectivity must be through an identified Electronic Access Point pursuant to CIP-005-5 Requirement R1 Part 1.2.
- Additionally, CIP-005-5 R1 Part 1.4 obligates Registered Entities to perform authentication for establishing Dial-up connections to high and/or medium impact-rated BES Cyber Systems, where technically feasible. The broad reference to system-to system remote access (which is silent to Dial-up) in combination with the absence of the provision for technical feasibility within this draft Requirement is effectively and expansion in scope to the already approved and enforceable CIP-005-5 R1 Part 1.4 Reliability Standard. Any expansion in scope to remote access requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-005-5 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the

creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-005-5 R1 Part 1.4 through a CIP Senior Manager and regional regulator approved Technical Feasibility Exception becomes a matter of non-compliance pursuant to CIP-013-1 R4.

CIP-005-5 R2 Parts 2.1 – 2.3 and CIP-007-6 R5 Parts 5.1 goes beyond in addressing CIP-013-1 R4(ii), R4.1, ultimately rendering CIP-013-1 R4(ii), R4.1 superfluous and unnecessary in that:

- CIP-005-5 R1 Parts 2.1 mandates authorization for all Interactive Remote Access (IRA) (including vendor-initiated IRA) through the requirement to use an Intermediate System such that any remotely-initiated IRA does not directly access the high and/or medium impact-rated BES Cyber System(s),
- where those Intermediate System must also utilize encryption that terminates at the Intermediate System pursuant to CIP-005-5 Requirement R2 Part 2.2, and
- where all IRA sessions must require multi-factor authentication pursuant to CIP-005-5 Requirement R2 Part 2.2.
- CIP-007-6 R5 Parts 5.1 further mandates methods to enforce authentication of interactive user access (including vendor-initiated users) where technically feasible for high and/or medium impact-rated BES Cyber System(s),

CIP-005-5 R1 Parts 1.2 - 1.5, in combination with CIP-007-6 R4 Parts 4.1-4.4 and CIP-007-6 R5 Part 5.7 collectively addresses, and in some cases exceeds, the logging, monitoring, and detection of unauthorized activity proposed in CIP-013-1 R4, R4.2, ultimately rendering in CIP-013-1 R4, R4.2 superfluous and unnecessary in that:

- CIP-005-5 R1 Part 1.5 mandates one or more methods for detecting known or suspected malicious communications both inbound and outbound on the Electronic Access Points protecting high and/or medium impact-rated BES Cyber System(s), and because all remote access must also be through an identified Electronic Access Point pursuant to CIP-005-5 Requirement R1 Part 1.2, the two existing enforceable requirements in combination already satisfying the detection component intended by CIP-013-1 R4, R4.2; and consequently, the detection component intended by CIP-013-1 R4, R4.2 adds no security or reliability value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-005-05 R1.
- CIP-007-6 R4 Parts 4.1-4.4 mandates that, per BES Cyber System capability or at the Cyber Asset level for high and/or medium impact-rated BES Cyber System(s),
  - specified access-related events are logged,
  - alerts are generated for said events,
  - event logs are retained as technically feasible for 90 consecutive calendar days except in CIP Exceptional Circumstances,
  - thereby already satisfying the logging and monitoring component intended by CIP-013-1 R4, R4.2; Consequently, the logging and monitoring component intended by CIP-013-1 R4, R4.2 adds no security or reliability value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-007-6 R4 that is also at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.
  - Furthermore, in its redundancy of CIP-007-6 R4, CIP-013-1 R4, R4.2 is simultaneously an expansion in scope in that CIP-013-1 R4, R4.2 is silent to the provisions for “Per Cyber System capability”, per cyber Asset capability”, “technical feasibility”, and “CIP Exceptional Circumstances”, is effectively and expansion in scope to the already approved and enforceable CIP-007-6 R4 Reliability Standard. Any expansion in scope to logging, monitoring, or detection activity related to requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-007-6 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-007-6 R4 through:

- a CIP Senior Manager and regional regulator approved Technical Feasibility Exception,
- a CIP Senior Manager approved CIP Exceptional Circumstance,
- a documented per BES Cyber System incapability, and/or
- a documented per Cyber Asset incapability

becomes a matter of non-compliance pursuant to CIP-013-1 R4.2

- CIP-007-6 R5 Part 5.7 mandates limiting of the number of unsuccessful authentication attempts or the generation of alerts of unsuccessful authentication attempts exceeding a Registered Entity defined threshold, where technically feasible and scope to high impact BES Cyber Systems and medium impact BES Cyber Systems at Controls Centers. The broad reference high and medium impact BES Cyber Systems, in combination with the absence of the provision for technical feasibility within this draft Requirement for CIP-013-1 R4 is effectively and expansion in scope to the already approved and enforceable CIP-007-6 R5.7 Reliability Standard. Any expansion in scope to logging, monitoring, or detection activity related to requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-007-6 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-007-6 R5 Part 5.7 through a CIP Senior Manager and regional regulator approved Technical Feasibility Exception becomes a matter of non-compliance pursuant to CIP-013-1 R4.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3

Answer	No
Document Name	

Comment

OUC requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. OUC requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. OUC requests changing the language to “upon detected unauthorized activity”.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
The Technical Guidance and Examples state that “for Requirement R4 Part 4.1, an entity may already have some authorization controls in place that will support meeting this objective”, including CIP-004 and CIP-007 R5 controls if they are fully implemented for vendor-initiated Interactive Remote Access. Please confirm that implementation of these controls for all remote access, vendor or entity initiated, would meet compliance with this requirement. If so, would it be beneficial to caveat the requirement and have it read “**4.1** Authorization of remote access, not previously approved by CIP-004, by the Responsible Entity?” A responsible entity may have numerous contractors from various vendors that perform a number of tasks within CIP environments that are on-site, sitting right next to employees engaged in similar activities. Both the contractors and the employees normal work process may have them utilize Interactive Remote Access to perform their responsibilities efficiently. Are these contractors, embedded and onsite, to have each of their connections explicitly approved and monitored at a different level of scrutiny than actual employees of the responsible entity, simply because they are not employees? Or will there be a distinction between on-site and off-site “vendors?”	
Likes 0	
Dislikes 0	

Response
Steven Rueckert - Western Electricity Coordinating Council - 10
Answer	Yes
Document Name	
Comment
R4 could give entities the impression that they do not need to follow the CIP-005-5 R2 controls for Interactive Remote Access. If an entity did not leverage its existing Interactive Remote Access (CIP-005-5 R2) processes to support this Requirement, WECC is concerned that separate vendor remote access processes may provide additional ingress/egress points into the ESP. An entity should ensure that vendor remote processes are protected at least to the level of CIP-005-5 R2. At no point in time, should there ever be an unmonitored connection into a BCS. This is something that is totally under the control of the entity. Even if the vendor includes a "phone-home" feature on a system or application, the ingress and egress of that connection should still be monitored and controlled by the entity to minimize the risk of third-party penetration into the BCS. The SCRM team should work closely with the CIP-005-5 team to ensure all remote access connections are managed, monitored, and controlled through an Electronic Access Control and Monitoring System [EACMS] and/or Intermediate System [IS]
Likes 0	
Dislikes 0	
Response
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable
Answer	Yes
Document Name	
Comment
While in overall agreement with this Requirement R4, ACEC would recommend the following change: 1. Move Requirement 1, Part 1.2.2, "Process(es) for notification when vendor employee remote or onsite access should no longer be granted" and Part 1.2.6 "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)" to Requirement R4 since this requirement is where Vendor Remote Access is addressed.
Likes 0	
Dislikes 0	
Response
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer	Yes
Document Name	

Comment
This appears to meet the FERC directive.

Likes 0	
Dislikes 0	

Response

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	

Comment
No additional comments.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	

Comment
We recommend the SDT address CIP Exceptional Circumstance with respect to this requirement aligned with project 2016-02. Also please see our earlier comments with regards to redundancy between R4 and R1.2.6.

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • Recommend changing Requirement 4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to detected unauthorized activity associated with remote access sessions.“ PSEG finds that inclusion of the word “during” in the requirement overreaches the intent of relevant FERC directive (p.51). • Requirements R1 and R2 do not require the registered entity to go back and revise previous contracts. In order to comply with this requirement, R4, past contracts / vendor service agreements may be required. Alignment is needed between R1, R2, and R4. • Vendor-initiated Interactive remote access is no different than Interactive remote access. Recommendation to incorporate Requirement R4 into CIP-007 R5 System Access Control. • Requirement R4 overlaps with CIP-005 for Interactive Remote Access, which applies to vendors, only 4.2 monitoring and 4.3 is new. Recommend streamlining R4 to fit in CIP-005 R2. • Recommend changing “activity” to “access”. Use of the word “activity” in 4.2 and 4.3 because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. In almost all cases, the vendor has more in depth technical knowledge of the system they developed beyond the Registered Entity’s level of expertise on the system. Therefore it would be difficult for the Responsible Entity to recognize inappropriate actions/activity. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. If the intent of this requirement is to monitor “unauthorized activity”, the term “unauthorized activity” should be defined.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	

Comment
AZPS requests changing Requirement R4.3 to read ‘disabling or otherwise responding to **detected,** unauthorized activity during remote access session’. It further notes that, as written, the proposed Requirement R4 would place Registered Entities in “double jeopardy” where similar controls are already required under CIP-004-6. Accordingly, AZPS requests that the SDT consider revising this requirement to remove such redundancy or to include a clarification regarding how this risk for “double jeopardy” will be managed relative to access controls required under CIP-004-6.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wes Wingen - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
George Tatar - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	

Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	

Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	No
Document Name	

Comment

The NSRF does not understand the intent of the following:

R1 is applicable to “Each Responsible Entity” is to implement “one or more supply chain risk management plans”.

R2 is applicable to “Each Responsible Entity” is to review and update its “supply chain risk management plans” at least once every 15 calendar months.

R5 is applicable to “Each Responsible Entity” with at least one “low impact BES Cyber System” will have a documented “cyber security policies “ which require “review and approval” at least once every 15 calendar months.

For R5.1, imposes a requirement at the BES Cyber Asset level rather than at the BES Cyber System level. Consider removing R5.1 or reworking so it is applicable at the BES Cyber System level.

The NSRF has concerns with R5. As written, every entity with a “low impact BES Cyber System” is required to have “cyber security policies” (note policies should be changed to “policy(s)). This would include entities that have High and Medium impact BES Cyber Systems, as long as they have one “low impact BES Cyber System”, too. Plus, R5.1 is a duplicate of R3 and R5.2 is a duplicate of R1.2.6.

This will cause double jeopardy for Each Responsible Entity in R1, R2, and R5. The “Responsible Entities” statement within each Requirement contains “High, Medium, and Low BES Cyber Systems”. So everywhere “Responsible Entity” is used in the Standard, that requirement applies to everyone with High, Medium, and Low BES Cyber Systems.

The NSRF believes that this is NOT the intent of R5. If the intent of R5 is to have control for Entities with “low impact BES Cyber Systems” **only** then, it should be clearly stated. Such as:

*“R5. Each Responsible Entity with at least one asset identified in CIP-002, containing low impact BES Cyber Systems **only,** shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:”*

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	No
Document Name	
Comment	
Requirement 5.1 needs to be removed. Currently patching is not required as a function for low impact assets. Until vulnerability and patching is made a requirement for low impact assets, then it is not possible to ensure that “all” patches for low impact assets be validated for authenticity. Additionally, given the issues with trying to validate authenticity for software and patches in general (see our comments on R3) then this sub-requirement cannot be enforced. The sub-requirement for remote access is valid and should be implemented for low impact assets.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn’t clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
R5 requires a Policy for Low Impact BES Cyber Systems. The two sub requirements are more plan based than policy based and would recommend making them an addition to CIP-003-7(i) attachment A instead. This will keep all LOW Impact BES Cyber Asset requirements in one location.	
Likes 0	

Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	

Comment
R5 fundamentally does not work as a low-impact scale-back of R3 and R4, because it can be meaningfully implemented only on a Cyber Asset level, and CIP-002-5.1 (R1.1.3) and CIP-003-6 (R2) do not require identification of Cyber Assets for low-impact BES Cyber Systems. The entire concept of R5 needs revision. The difference between supply chain risk management policies, as called-for in R5, and processes, mandated in R3 and R4, is unclear. TFE opportunity is again needed, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses).

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	

Comment
See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5	
Answer	No
Document Name	

Comment

AEP is concerned about low impact BES Cyber Systems being included here because it may incentivize a lack of action on those systems in order to avoid compliance obligations. AEP believes the Standard should be reasonable for all to achieve, and this may create a significant recordkeeping burden for low impact systems. R5, as proposed, only requires a “documented policy”. Responsible entities could manage the risk appropriately for their circumstances without a requirement to “implement”.

Likes 0	
Dislikes 0	

Response

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3

Answer	No
Document Name	

Comment

See comments to Question 1.

These should clearly be modifications to CIP-003-7(i) Attachment A, and not lumped into CIP-013, Supply Chain Risk Management.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

These risks should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-005 R2 and CIP-007 R2.

IID does not agree with including Low Impact BES Cyber Systems in this standard as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. The SDT would need to clarify measures that would serve as evidence. As mentioned above, if the SDT feels that gaps remain, SRP feels that the modifications should be made in the standard where the topic is already addressed (CIP-003).

Additionally, IID feels that there should be exclusion comparable to a CIP Exceptional Circumstance (or TFE) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The current CIP requirements for BCS at low impact sites do not require identification of patch sources, or other patching procedural controls. Introducing R5 inadvertently requires utilities to develop a CIP-007 R2 program for low sites as well to be able to address software integrity. This policy would also require a software list and inventory of systems to provide evidence that the policy has been followed. Implementing CIP-013 essentially applies controls from CIP-005, CIP-007, CIP-008, and CIP-010 to BCS at low impact sites where there are no corresponding requirements within the existing CIP standards. For example, it is incongruous to require verification of patches on a low BCS for which there is no requirement to patch.	
Likes 0	
Dislikes 0	
Response	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	No
Document Name	
Comment	
Smaller generation facilities are heavily dependent on the Original Equipment Manufacturers, and do not have the leverage to promote participation from large sole sources. How do facilities develop processes to verify integrity and authenticity of software and firmware, when OEMs don't offer guidance on validation? The sole sources also do not have the incentive to adhere to the same level of compliance when these assets are in their care, such as when embedded cyber assets are shipped off site to the OEM, or when service engineers are on site for commissioning. Enhanced compliance requirements discourages equipment servicing from the owner, and places more reliance on the OEM.	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends the deletion of this requirement. As stated in our comments earlier, based on the minimal threat to stability that Low Impact BES Cyber Systems pose to the BES, coupled with the lack of an inventory list for said Low Impact systems to demonstrate compliance, we feel that this requirement is unnecessary and impossible to effectively demonstrate compliance to.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Requirement R5 speaks to documenting a policy or policies to address 5.1 and 5.2 for low impact BCS. The word “implement” is not in this requirement. Absent including the implementation piece, there is no requirement to implement the controls just document them.

Furthermore, the SDT made it clear in Requirement R3 and R4 that an entity shall implement one or more documented process(es) for the actual security controls or processes. Similar language (implement documented process(es)) should be included in R5 versus policy. Even though the rationale section speaks to policies and processes, the language of the requirement only speaks to policies. This will drive consistent implementation across all BCS impact levels. ReliabilityFirst offers the following modifications for consideration to address our concern:

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall [implement] have one or more documented cyber security policies [or processes], which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	

Answer	No
Document Name	

Comment

We request consistency in the use of terms between R1 and R5; R1 uses the term “plan” and R5 uses the term “process” or “policy”. We understand the term “plan” to mean a more high-level document that communicates management goals and objectives. We request clarification that the use of the term “policy” in R5 is meant to be a similar concept, i.e., that R5 is satisfied by a document that is reviewed and approved by the CIP Senior Manager that is a high-level document that communicates management goals and objectives, rather than a detailed process document with instructions to achieve the requirements. We seek this clarification because in the Technical Guidance and Examples (page 16 lines 29-31), the SDT writes “or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber System.” As described previously by the Version 5 SDT, a documented process and a policy are two different documents: a policy is a document used to communicate management goals and objectives, while a process is a set of required instructions specific to achieving the requirement. Based on the SDT’s comments in the Technical Guidance and Examples, it is unclear which will satisfy R5 and how it will be audited.

Clarification is also requested on whether “system to system” access applies to access that is “one-way” where the remote end conducts only monitoring activity and no control is possible. Can the procedure for access make distinctions for each methods of monitoring each type of access, Interactive Remote, system to system with control and system to system for monitoring only?

Additionally, we request confirmation that if vendors refuse or can’t provide hashes or other verification methods, an internal process to test, scan and perform verification activities be enough to satisfy requirement R5.1.

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

ALAN ADAMSON - New York State Reliability Council - 10

Answer	No
Document Name	

Comment

See NPCC Comments.

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No

Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI has concerns that R5, as written, would place Responsible Entities that have a combination of High, Medium, and low impact BES Cyber Systems at risk of double jeopardy. Part 5.1 is a duplicate of R3 and R5.2 is a duplicate of R1.2.6. This requirement should be removed from CIP-013-1 and addressed in CIP-003, R2, Attachment 1.	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	No

Document Name	
Comment	
PRPA is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. PRPA requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, PRPA requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	
AE is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. AE requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, AE requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No

Document Name	

Comment

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003.

R5.1 is not consistent with R1.2.5, should R5.1 include the term “that are intended for use” to read “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and”

Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls R5 needs to be a process not a policy. If this is a policy, then suggest removing “controlling”

There should be exclusion comparable to a CIP Exceptional Circumstance added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy. R5 should be a plan document and not a policy document.

Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No

Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
CIP-013-1 R5 should be placed within CIP-003 in order to keep consistency with the approach used in the remaining CIP standards. Low impact requirements were placed in CIP-003 in order to keep all requirements within a single standard and requirement. By adding these requirements into a new standard, there is confusion resulting in an increased likelihood of a violation. Guidance language should be added for the auditing process within the standard's guidelines and technical basis (not in a separate document). Not including this in the standard places no obligation on the auditors. Without this guidance language, the auditors could choose to audit in a near zero defect manner, as opposed to a quality of program manner. Providing clear guidance sets expectations for the entities.	
Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. SRP requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, SRP requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Response	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	

- This Requirement should be removed from the Standard. For consistency with the other CIP Standards (e.g. compare to the current draft revision of CIP-003-7i standard where Transient Cyber Asset language for assets that contain Low Impact BCS is included) applicability of supply chain risk management to assets that contain Low Impact BCS should be consigned to CIP-003, R1.2 and R2:
    - R2 – Attachment 1 should be expanded to include a Section for supply chain risk management (to include controls on software authenticity for Low Impact BCS, controlling vendor remote access to Low Impact BCS)
    - R1.2 – should be expanded to include supply chain risk management plan(s) with controls for assets that contain Low Impact BCS
- The NERC Glossary of Terms definition of CIP Senior Manager will require update to include CIP-013

Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Mike Kraft - Basin Electric Power Cooperative - 5

Answer	No
Document Name	

Comment

Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013.

For R5.1, imposes a requirement at the BES Cyber Asset level rather than at the BES Cyber System level. Consider removing R5.1 or reworking so it is applicable at the BES Cyber System level. Basin Electric is concerned R5.1 will necessitate maintaining a list of low BES Cyber Systems and possibly a list of low BES Cyber Assets.

Basin Electric suggests modifying the requirement to include clarification of when the obligation starts. Perhaps add language to the front of R5 such as: "For assets containing low impact BES Cyber Systems in production…"

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1. R5 will be the only low impact specific requirement not to be in CIP-003.

Concerned that in R5.2 the term "controlling" is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing "controlling"

CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

Does R5 allow the Entity to “accept the risk?”

R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment

See comments on Requirement R5 in attached file.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes it is inappropriate to try to define what amount to electronic access control requirements (vendor remote access) while revised electronic access control requirements in CIP-003 have not yet been formally approved.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
As we reviewed Requirement R3 and Requirement R4, it is our understanding that a Management Plan needs to be developed and maintained. However, Requirement R5 is requiring security policies. At this point, we feel that there are inconsistencies in the Requirement language as well as potential Compliance Enforcement issues in reference to those particular Requirements. We would ask the drafting team to provide clarity on why Requirement R3 and Requirement R4 mentions Management Plans and Requirement R5 mentions security policies. Additionally, the proposed language in Requirement R3 and Requirement R4 mentions high and medium Impact BES Cyber Systems. Requirement R5 mentions Low Impact BES Cyber Systems. Again, we would ask for clarity on why all three (3) Cyber Systems type aren't included in Requirement R3 through Requirement R5? Finally, we suggest revising Requirement R5 language and moving it to the CIP-003 Standard. In the case that the drafting team doesn't agree with the revising of the Requirement's language, Our group recommends that this Requirement language be moved to the CIP-003 Standard because, we feel that it's the most appropriate Standard to handle this Requirement which is applicable to Low Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	
Comment	

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1

Answer	No
Document Name	

Comment

Exelon has the same concerns regarding the lack of a compliance “safety valve”, the potential for double jeopardy as well as the administrative burden of updating the supply chain cyber security risk management plan(s) for newly identified vulnerabilities as included in the comments on R1-R4. The discussion under (4) identifies how the proposed R5 overlaps with existing CIP Standards.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We agree with EEI's recommendation to delete R5.

Part 5.2 is duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

Extending the operational controls for authenticity/integrity in Part 5.1 to low impact BES Cyber Systems is not commensurate with the risk. If the SDT thinks the risk to low impact BES Cyber Systems is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing the massive scope of these low impact systems.

NERC's Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets, but very different risks.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Dominion is of the opinion that all CIP policy requirements should be located in CIP-003 and that all requirements for low impact BES cyber assets should be placed in Attachment 1 of CIP-003. Placing all of the low risk operational CIP requirements in a single standard allows entities that have only low impact cyber assets to reference a single source for pertinent requirements.
- Dominion recommends the following modification to Part 5.1:

5.1: Verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to authorized installation into a low impact BES Cyber System."

- Dominion recommends the removal of Part 5.2. Access control obligations, including system-to-system remote access already exist in Section 3 of Attachments 1 and 2 of CIP-003-7 for low impact. CIP-003-7 is currently pending FERC approval.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

With the applicability of low impact BES Cyber Systems, this appears to negate a comment in CIP-002, R1.3 where it states, "… (a discrete list of low impact BES Cyber Systems is not required)".

What is the timing of R5.1 in terms of new software and existing software? The rationale explains that this starts in the operate/maintain phase of the life cycle but does the timing/life cycle language need to be added to the Standard rather than explained in the rationale section, which may not appear in the final language? Does this apply only to devices in production? For example, what if software is pre-loaded by an OEM. Is there an expectation that the Regional Entities work with their OEM to verify integrity and authenticity prior to this pre-loading? We seek more clarity in the language of R5 and recommend adding "…for Cyber Assets in production."

Regarding the security controls for vendor initiated and system-to-system remote access, R5 is about one or more documented policies and R4 is about the processes for authorization, logging and monitoring, and de-provisioning of remote access. With the requirement of one or more documented cyber security policy, how would Responsible Entities enforce the policy(ies) without also requiring documented plan(s) and process(es), which R5 does not address?

There is no need to have R5 because coverage of low impact BCS is already included in R1. There are two options for R5: integrate it into either (1) existing applicable NERC CIP Standards or (2) R2, R3, and R4 of CIP-013-1.

For option #2:

R2 is about the periodic review and approval of the supply chain cyber security plan(s) developed in R1. R3 obligates Entities to define process(es) to verify the baseline components and any upgrades prior to BCS installation. Requirement R5.1 appears to be identical to R3 because the term "software" in R5.1 is broad in scope and includes the OS and commercially available or open source software.

If Entities are concerned with R4.2 for low impact BCS, the integration of R5 and R4 can either include (1) "per Cyber Asset capability" or "if technically feasible" language for low impact devices or (2) specific language of a risk-based approach, vendor or system, in determining where remote access controls will be applied.

We recommend option #1, the removal of R5 from CIP-013-1 and integration of the requirement into existing applicable NERC CIP Standards.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

R5 discusses a Low policy – NRG recommends that this requirement should be moved to the CIP-003-7i standard where all CIP policy requirements are outlined.

As we reviewed the Requirements applicable to Requirement R3 and Requirement R4, it is to our understanding that a Management Plan needs to be developed and maintained. However, Requirement R5 is requiring security policies. At this point, we feel that this creates inconsistencies in the Standard language as well as potential Compliance Enforcement issues in reference to those particular Requirements (jumping from plans to a policy).

For SDT consideration, there is no access control requirement today for Low Impact Interactive Remote Access which expands the scope broadly to existing CIP standards. This is a similar concern for patching updates (patch management) for Low Impact BCS.

NRG is concerned that in R5.2 the term "controlling" implies operational and technical controls which is inconsistent with a policy level requirement.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

9. Does R5 allow the Entity to “accept the risk?”

10. R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

11. Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	

Same as RoLynda Shumpert's comments from SCE&G:

With the applicability of low impact BES Cyber Systems, this appears to negate a comment in CIP-002, R1.3 where it states, "… (a discrete list of low impact BES Cyber Systems is not required)".

What is the timing of R5.1 in terms of new software and existing software? The rationale explains that this starts in the operate/maintain phase of the life cycle but does the timing/life cycle language need to be added to the Standard rather than explained in the rationale section, which may not appear in the final language? Does this apply only to devices in production? For example, what if software is pre-loaded by an OEM. Is there an expectation that the Regional Entities work with their OEM to verify integrity and authenticity prior to this pre-loading? We seek more clarity in the language of R5 and recommend adding "…for Cyber Assets in production."

Regarding the security controls for vendor initiated and system-to-system remote access, R5 is about one or more documented policies and R4 is about the processes for authorization, logging and monitoring, and de-provisioning of remote access. With the requirement of one or more documented cyber security policy, how would Responsible Entities enforce the policy(ies) without also requiring documented plan(s) and process(es), which R5 does not address?

There is no need to have R5 because coverage of low impact BCS is already included in R1. There are two options for R5: integrate it into either (1) existing applicable NERC CIP Standards or (2) R2, R3, and R4 of CIP-013-1.

For option #2:

R2 is about the periodic review and approval of the supply chain cyber security plan(s) developed in R1. R3 obligates Entities to define process(es) to verify the baseline components and any upgrades prior to BCS installation. Requirement R5.1 appears to be identical to R3 because the term "software" in R5.1 is broad in scope and includes the OS and commercially available or open source software.

If Entities are concerned with R4.2 for low impact BCS, the integration of R5 and R4 can either include (1) "per Cyber Asset capability" or "if technically feasible" language for low impact devices or (2) specific language of a risk-based approach, vendor or system, in determining where remote access controls will be applied.

We recommend option #1, the removal of R5 from CIP-013-1 and integration of the requirement into existing applicable NERC CIP Standards.

Likes 0	
Dislikes 0	
Response	

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	

We propose the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

2) If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

3) Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

4) R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

5) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

6) Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

7) CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

R5 modifies requirements for the Cyber Security Policy, in conflict with CIP-003 R1. It also modifies the approval level required for a Cyber Security Policy (Senior Manager ONLY), allowing a delegate to approve part but not all of a Cyber Security Policy. The entire requirement belongs in CIP-003 and should be reworded to not undermine the governance structure set out in CIP-003 and the authority of the CIP Senior Manager.

CenterPoint Energy recommends that the SDT consider moving the portion of this requirement that is not duplicative to CIP-003 with the rest of the requirements for assets that contain Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	

Comment
OUC is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. OUC requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, OUC requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	

Comment
CIP-003-6 R1.2 prescribes policy level controls. CIP-013-1 R5 effectively expands the requirements for policy beyond what is mandated in the current approved and enforceable version of the CIP-003-6 Reliability Standard. Any expansion in scope to CIP-related policy requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. CIP-003-6 R2 requires registered Entities to develop and implement plans for the control of electronic access (which includes remote vendor-initiated user or system-to-system access) thereby rendering CIP-013-1 R5.2 superfluous and unnecessary, as well as placing it at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value. CIP-003-6 R2 Attachment 1 Section 2 necessitates the implementation of electronic controls for low impact BES Cyber Systems in accordance with the plans developed pursuant to CIP-003-6 R2, thereby further rendering CIP-013-1 R5.2 superfluous and unnecessary, as well as placing it at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

CIP-002-5 Requirement 1 R1.3 explicitly excludes the requirement for an inventory of low impact BES Cyber Assets through the its parenthetic clause stating, "**a discrete list of low impact BES Cyber Systems is not required**" and CIP-013-1 R5.1 effectively expands this current approved and enforceable requirement through its detailed Cyber Asset-level expectation related to software and firmware and any patches, updates, and upgrades to software and firmware. Any expansion in scope to policy requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	

Comment

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	No
Document Name	

Comment
1. Supply chain risks may include insertion of counterfeits, unauthorized production, tampering and theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the industrial supply chain. Threats and vulnerabilities created by malicious actors (individuals, organizations, or nation states) are often especially sophisticated and difficult to detect, and thus provide a significant risk to organizations. It is difficult to understand how a low impact entity will be able to detect these risks and protect themselves against code that they have no control over. ACES recommends an approach that allows the vendors a process to communicate with low impact entities on how their product is secure. The vendor should be the focal point not low impact entities who do not have the resources to interact with multiple vendors constantly.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	

Comment
Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016. Reclamation recommends that Requirement R5 be deleted. There would be no need for Requirement R5 if all aspects of the supply chain risk management plan(s) are to be addressed in Requirement R1 and its sub-requirements.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	

Comment
Rationale for Requirement R5: The rationale language for R5 states, “An entity could apply process(es) used for Requirements R3 and R4 to satisfy its obligations in Requirement R5.” IPC does not see this language reflected in the R5 requirement language. If documented processes are an acceptable means of achieving compliance with R5, IPC suggests rewriting the R5 requirement language to include the terms “processes” or “policies.” Additionally, there is continued creep in the standard language (here and elsewhere) to add requirements for Low Impact BCS, when Responsible Entities are still explicitly not required to have an inventory of Low Impact BCS. If it is the intent of the SDT and regulators to continue adding requirements to Low Impact BCS, IPC recommends a re-

write of CIP-002-5.1 to ensure that all Low Impact BCS are appropriately identified rather than using standards to disagree with current enforceable standard language.

R5

The language of R5, R5.1, and R5.2 state, "Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

"**5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and

"**5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)."

IPC does not feel CIP-013-1 is an appropriate standard to address R5, R5.1, and R5.2. IPC believe R5, R5.1 and R5.2 belong in CIP-003-7(i), as R5, R5.1, and R5.2 are related to cyber security policies and low impact BES Cyber System requirements. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-003-7(i) addresses cyber security policies (High, Medium and Low) and all low impact BES Cyber System requirements.

IPC feels the requirement to have a policy reviewed by the CIP Senior Manager or delegate is purely administrative and does not provide value and recommends that it should be removed.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Santee Cooper requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, Santee Cooper suggests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

This requirement should be placed within CIP-003 alongside other requirements applicable to Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA recommends moving R5 to CIP-003 as it applies to Lows only. This will maintain the single standard requirement for entities that only have Low assets. The application of the requirement is not aligned with the current Low Impact BES Cyber System standard CIP-003 that does not require an inventory of equipment and software or identifying system cyber assets. Language and scope should be modified to provide clear scope and compliance requirements.

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003.

2) R5.1 is not consistent with R1.2.5, should R5.1 include the term “that are intended for use” to read “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and”

3) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls R5 needs to be a process not a policy. If this is a policy, then suggest removing “controlling”

4) There should be exclusion comparable to a CIP Exceptional Circumstance added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

5) R5 should be a plan document and not a policy document.

Likes 0	

Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	

Comment
CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	

Comment
Colorado Springs Utilities (CSU) is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CSU requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CSU requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	

Comment
Seattle City Light is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Seattle City Light requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, Seattle City Light requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	

Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
It is unclear how the risk and requirements in R5 for Low Impact BES Cyber Systems are differentiated from the other requirements and how the requirements will be measured considering a list of Low Impact systems are not required. There seems to be some reduncancy between R1 and R5 for Low Impact. Suggest removing Low Impact requirements from CIP-013 and incorporating into CIP-003 for consitency.	

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1

Answer	No
Document Name	

Comment

Why not address this as part of the Cyber Security policy for Low Impact in R1.2 of CIP-003?

Also what about the Cyber Security Policy for Highs and Mediums? Should that also address Supply Chain?

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. SMUD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, SMUD requests that all requirements related to low impact assets be included in CIP-003.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

We recommend that the SDT consider deleting Requirement R5.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

In addition, it should be noted that CIP-003 R2 requires a plan, while CIP-013 R5 requires a policy. Where LPPC's comments request "that all requirements related to low impact assets be included in CIP-003," this can be accomplished by having the policy language as a portion of CIP-003 R1 part 1.2.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
This requirement should be placed within CIP-003 alongside other requirements applicable to Low Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

We recommend that the SDT consider deleting Requirement R5.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

We recommend that the SDT consider deleting Requirement R5.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

We strongly disagree with requirement R5. The issues with this requirement are too many to list. In particular the SDT should avoid developing mandatory requirements that will reduce the security and reliability of the Bulk Electric System as it has proposed in this instance.

The directive in FERC Order 829 is limited to “the context of addressing supply chain management risks.” According to the definition of supply chain provided in NIST-800-53 (and referenced by FERC in paragraph 32, footnote 61), supply chain ends at the “delivery of products and services to the acquirer.” In the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur “upon commissioning” for planned system installations (and even later for unplanned changes). Therefore, this BES Cyber System identification, nor its categorization as low impact, does not exist during the supply chain context.

Further, no list of low impact BES Cyber Systems is required. In order to demonstrate compliance with R5, entities would need a list of low impact BES Cyber Systems along with a full system baseline. The net effect of this requirement will be a SIGNIFICANT reduction in security by providing a regulatory disincentive to patch known security vulnerabilities in low impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Response	

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

The expectations for R5.1 are out of Entity scope for the reasons stated challenging R3. However, Low Impact BCS software and firmware should be expected to be checked for functionality by the Entity.

Likes 0	
Dislikes 0	
Response	

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No

Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
As this Standard is supposed to be focused on the vendor and as supply chain management risks apply equally to all categorizations of BES Cyber Systems, these requirements are superfluous. Requirement R1 already applies to all BES Cyber Systems and includes these requirement elements. There is no reason to call out requirements specific to Low Impact BES Cyber Systems. If the elements of the plans and processes are vendor-focused as they should be, there is no need to itemize the Low Impact BES Cyber Systems, which is the apparent real reason for Requirement R5 being defined separately.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No

Document Name	

Comment

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

2) If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

3) Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

4) R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

5) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

6) Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

7) CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

· Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.

· To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

Does R5 allow the Entity to “accept the risk?”

R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Response

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6

Answer	No
Document Name	

Comment

This requirement implies larger burdens on Low Impact BES Cyber Systems than the upcoming CIP-003-7 changes in regards to patch management and tracking. In neither of the previous versions of CIP-003, was it deemed necessary for patch management controls to be applied to Low Impact BCS. The nonvariable nature of the phrase "…and **any** patches, updates, and upgrades…" states that the Policies implemented to address this requirement will require a validation on every asset with a Low Impact rating. We recommend removing this Requirement and addressing the FERC Directive solely through R1.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	
Comment	
The expectations for R5.1 are out of scope for and Entity for the reasons stated disputing R4. Low Impact BCS software and firmware should be expected to be checked for functionality by the Entity.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes all Low Impact BES Cyber System Controls should go into CIP-003 R1.2, not create a new Requirement under CIP-013.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	

Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 5.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
As currently written, R1 and R5 are applicable to low impact BES Cyber Systems. R5 requires "one or more documented cyber security policies" while R1 requires "one or more documented supply chain risk management plan(s)". CIP-003 requires first a policy and then a plan. Policies are typically higher level documents than plans so consistency is an issue here. R5 is duplicative of the review and approval by CIP Senior Manager required in R2. For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months and removed from CIP-013-1. R5.1 indicates a protection that needs to be applied at the Cyber Asset level, yet R5 is applicable to BES Cyber Systems. This language elevates low impact BES Cyber Systems to the level of medium and high impact BES Cyber Systems. Under existing CIP Standards, Security Patch Management requirements reside in CIP-007 and none are applicable to low impact BES Cyber Systems. Additionally, software and patching typically occurs at the Cyber Asset level and low impact entities are only required to identify assets containing low impact BES Cyber Systems. Implementing R5 applies controls from existing CIP Standards which are not applicable to low impact BES Cyber Systems. It is incongruous to require verification of patches on a low impact BES Cyber System for which there is no requirement to patch. For consistency purposes, this requirement should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to have a single place to for security plan requirements.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No

Document Name	
Comment	

- Regarding R5.1, the Standard Drafting Team should clarify what is intended by “[I]ntegrity and authenticity.” This is an ambiguous term which can have different meanings.

- Regarding R5.1, vendor information is proprietary (contractually). Registered Entities should not be held accountable for compliance obligations in which they have no control of.

- Requirements pertaining to BES Low Impact Cyber Systems should be placed within CIP-003 Attachment 1 as originally intended.

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	

As drafted, R5 greatly increases the requirements for low impact BES Cyber Systems and completely ignores the H/M/L impact model. We feel there should be no such requirements for assets deemed to have a low impact on the BES, and that R5 should be struck entirely. If the SDT disagrees, then please clarify how implementation of these requirements would differ for low impact versus a medium or high impact system?

In addition, Tri-State is struggling to see how implementation of this requirement could be accomplished without a maintained inventory of low impact BES Cyber Systems, vendors, and software. This would be an incredibly substantial effort, that we believe the previous V5 drafting team understood well, which is why entities are not required to have a list of low impact BES Cyber Systems. Please clarify how an entity would carry out such policies while keeping with a low risk model.

Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	

Concur with EEI’s Position

Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
SVP agrees with other entities that requirements imposed on low impact assets be contained in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
NRECA recommends that CIP-013-1 R5 be placed within CIP-003 in order to keep consistency with the approach used in the remaining CIP standards. Low impact requirements were placed in CIP-003 in order to keep all requirements within a single standard and requirement. By adding these requirements into a new standard, there is confusion resulting in unnecessary compliance confusion.	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	No
Document Name	

Comment

This requirement should be eliminated in its entirety. We have adequate cyber controls in place for low impact Cyber Systems. The classification recognizes that these systems inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES.

Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

As with other comments, this requirement is duplicative and should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to refer to a single standard to for security plan requirements.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	No
Document Name	

Comment

Southern Company disagrees with the direction the proposed R5 requirement is taking, specifically with regard to the implied requirement to have a system baseline inventory of software and/or firmware on each Low Impact BES Cyber System when such an inventory is explicitly not required by existing CIP Standards. Not only does this create a collision of Standard requirements, but the burden on Responsible Entities would be immense and unmanageable – significantly increasing risk to reliability. Despite interpretation of language in this FERC Order, previous commission Orders have supported not requiring inventories at the Low Impact level. Southern recommends the comments previously provided under R1 to properly scope this Standard to “industrial control system” vendor products and services, within the Supply Chain horizon, where risk to assets containing Low Impact BES Cyber Systems is more appropriately addressed.

If the SDT chooses to keep R5 in the Standard in this manner, Southern provides the below edits to more appropriately scope this requirement towards the ICS vendor products at “assets containing lows.” Again, consideration must be given to modifying this requirement language in a manner that does not introduce an implied responsibility to maintain an inventory of Low Impact BES Cyber Systems, their member Cyber Assets, and/or the individual component software and firmware baselines of those System components.

For example, if an entity has a thousand or more substations, it does not require a device level inventory of all devices in all substations to know the few vendors of relays that would be in those substations. Therefore, the entity would need to document how they deal with the firmware upgrades for those vendors. The same goes for generating plants; the entity does not need to know the thousands of individual devices in a plant to know the DCS or

turbine control vendors per unit. Therefore, having plans and controls for dealing with the software, services, and remote access for those vendors is what is needed.

Additionally, Southern Company disagrees with the placement of this requirement, should it remain in this Standard, recognizing the SDTs time constraints with having to file a new or modified Standard addressing Supply Chain cyber security risks as per the FERC Order. Any requirement addressing controls for assets containing Low Impact BES Cyber Systems should be placed in CIP-003-6 R2, Attachment 1.

Modify R5 language as follows:

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics, based on risk, for its industrial control system vendor products and services at assets containing low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

5.1. Integrity and authenticity of software and firmware and any patches, updates,

and upgrades to software and firmware; and

5.2. Controlling vendor-initiated remote access, including system-to-system remote

access with vendor(s).

Likes 0	
Dislikes 0	

Response

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	No

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
The proposed application of specific requirements to Low Impact BES Cyber Systems in CIP-013-1, R5 appears reasonable.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
While in Agreement with the concept of adding a Requirement for low impact BES Cyber Systems, ACEC does have the following concerns: 1. Part 5.1 requires the Responsible Entity to have one or more cyber security policies for "Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware." This requirement is not consistent with CIP-002-5.1 which states in Requirement 1, Part 1.3 that "a discrete list of low impact BES Cyber Systems is not required." To be able to track security patches and firmware upgrades you will by necessity have to have a discrete list. It is recommended that Part 5.1 be replaced with the Information system planning security controls: this will ensure that security will be part of the planning for low impact Information Systems/Control Systems. 2. Part 5.2 requires the Responsible Entity to have one or more cyber security policies for "Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)." At present, CIP-003-6 Attachment 1, Section 3 requires only that you (3.1) "For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access;" and "Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability." This new Requirement extends these controls significantly beyond the present CIP-003-6 requirement and should be replaced with the Vendor risk management and procurement security controls: this will ensure that these issues are addressed early in the procurement process and throughout the lifecycle of low impact BES Cyber Systems and their associated Cyber Assets.	

3. This Requirement should be moved to CIP-003-6, where ALL low impact BCS Cyber Systems security controls are addressed. This will allow Registered Entities with only low impact BES Cyber Systems to address only CIP-002-5.1 and CIP-003-6, reducing the potential for confusion. This approach has been taken by SDT 2016-02 in adding Transient Cyber Assets/Removable Media requirements to CIP 003-6 vice including in CIP-010-2 where it is addressed for high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Should a reference to cyber security policies related to this Requirement for Low-impact BCS also be incorporated into CIP-003-7(i) R1.2?	
Likes 0	
Dislikes 0	
Response	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
In the VSL for Requirement R5 there is no recognition of a Responsible Entity that had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, but the approval was more than 18 calendar months. A third entry should be added to the Severe VSL for Requirement that reads: *The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however, the approval was more than 18 calendar months from the previous review.*	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes

Document Name	

Comment

AZPS understands the time constraints associated with the development of this proposed standard, but respectfully asserts that all policy-related obligations should be consolidated into the appropriate requirements of CIP-003. AZPS, therefore, recommends that, upon completion of this standards process, a SAR is entered to consolidate policy-related requirements such as Requirement R5 the existing CIP-003 Requirement R1.2

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

PSEG agrees with the intent of this requirement, but has the following questions/recommendations below:

- Recommend moving CIP-013 R5 to CIP-003 R1.2, to remain consistent with previous decisions to maintain all low impact requirements in CIP-003.

- Request clarification. Requirement R5 requires one or more documented policies. The Rationale for Requirement R5 states “An entity could apply process(es) used for Requirement R3 and R4 to satisfy its obligations in Requirement R5 or could develop a separate policy or processes to address low impact BES Cyber Systems.” Is the intent of R5 similar to R3/R4 that the outcome is “one or more documented processes”? If so, should there be a separate policy requirement added to CIP-003 to have the CIP Senior Manager approve the policy?

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Kenya Streeter - Edison International - Southern California Edison Company - 6	

Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
As the IESO does not have low impact Bes Cyber Assets we abstain from commenting on this requirement.	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Document Name	

Comment	
The IRC and SWG abstains from commenting on this requirement.	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

Dennis Sismaet - Northern California Power Agency - 6

Answer	No
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

In light of the sweeping changes represented by CIP-013, potentially altering the way an entire industry assesses risk, deals with vendors and contractors, and performs security operations tasks, the 1 year after FERC approval effective dates are far too short for implementation.

CenterPoint Energy would like to propose an effective date of at least 24 months following FERC approval. It will be a significant effort for entities to write a plan, negotiate with vendors, train and work with new groups to implement the requirements.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	No
Document Name	

Comment

1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

2) Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.

3) Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	No
Document Name	

Comment

Entergy seeks clarification on if the implementation date for CIP-013 merely requires that the entity have a CIP supply chain management plan in effect (with the ability to have a rolling implementation of specific protections and controls directed in that plan similar to the CIP-014 implementation), or if all protections and controls directed in the plan (including the potential technical deployment of new devices/systems) must be installed and live on day one of the implementation date. In other words, Entergy notes that the proposed standard recognizes and allows for a multi-phased, or rolling, implementation of the CIP supply chain management plan by not requiring contracts be renegotiated to adopt new terms and conditions; Entergy requests that CIP-013 explicitly allow entities to likewise have a phased or rolling implementation of identified controls and protections measures identified in their security plans after the implementation date.

In the alternative, Entergy cannot support the “12 month” implementation plan and recommends the date be no less than 18 months until more certainty on the extent of technical deployments required by the Standard can be provided. For example, until more clarity is given regarding whether implementation of existing CIP-005 and CIP-007 controls will adequately meet compliance with CIP-013 R4 and R5, or regarding the definition of “vendor remote access.” This is because, depending on the date of passage, the 12 month implementation requirement may fall outside of an entity’s capital planning and budgeting process, resulting in considerable constraints in acquiring funds for significant capital investment to achieve compliance with the standard.

Accordingly, Entergy requests that either a phased or rolling implementation be explicitly approved, or the implementation date be no less than 18 months.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	
Same as RoLynda Shumpert's comments from SCE&G: *With the inclusion of CIP-013 R1 through R5, SCE&G does not agree with the Implementation Plan. We agree with EEI's recommendation of extending the schedule from 12 months to 18 months.*	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	
R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems. Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.	

Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

The implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

In the implementation plan for this standard, NRG recommends a staggered implementation plan for R1, R2, & R5 being 15 calendar months. However, NRG recommends a 24-month implementation plan for R3 & R4would be needed for Registered Entities to manage this process on all impacted systems due to the need to re-negotiate processes with vendors (individualized solutions).

The implementation plan should have a timeline for compliance for initial enforcement and subsequent plan revisions – similar to CIP-002 with planned and unplanned changes.

In reference to R1 and contracts, we suggest that the term “future contracts” be addressed in the requirement language such as: “new or modified contracts” on or after the date of Enforcement. These should be vetted in an implementation plan. There will be a conversation of initial compliance versus implemented/ongoing compliance; therefore, NRG requests clear understanding of the implementation plan scope as it pertains to plan reviews, new contracts, modified contracts, and current contracts.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

With the inclusion of CIP-013 R1 through R5, SCE&G does not agree with the Implementation Plan. We agree with EEI’s recommendation of extending the schedule from 12 months to 18 months.

Likes 0	

Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Under General Considerations, additional language should be added to address existing contract extensions or addendums, effectively excluding them as well.

For the implementation plan which is 12 months, Dominion recommends an 18 month implementation period for the following reasons:

- Time is needed for entities to assess and impacted contracts relevant to applicable BES Cyber Assets.
- Budgets cycles often extend beyond a 12 month timeframe.
- New environments and assets may be in scope.
- This revision necessitate that entities conduct an impact assessment to determine what changes the revisions create and what is currently in place from the assessments performed for CIP version 6 implementation for low impact BES Cyber System.
- Revision iterations always require some time to assess and verify points of change.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

We do not support the implementation plan based on the proposed changes recommended in approach to addressing the directives. The implementation plan has to be revised to reflect a revised approach.

Implementation of operational cyber security controls changes to standards CIP-002 through -011 should provide for at least two years, especially because of the time it may take some entities if they have to completely revise how their vendors are currently providing service to them.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon generally agrees with the Implementation Plan for CIP-013-1 but offers the following recommendation for clarifying the plan for R2. The initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 must be completed within fifteen (15) calendar months **following** the effective date of CIP-013-1. There should be no obligation to review the plans ahead of time, and only the initial development and implementation should be required. This should be made clear in the Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes that 12 months from the Effective Date is too short for robust implementation. 18 months might be more appropriate.	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	

Resilient Societies recommends a strategic reassessment of how NERC should, in good faith, respond to FERC Order No. 829. Many of the cost-effective remedial initiatives will be beyond the control of the North American electric utilities industry. Fundamental changes in the procurement of IT and OT systems will be required. Also, there are promising cross-industry initiatives to develop Open Source Codes that will better protect industrial control systems and other control systems upon which the electric utility industry depends. NERC should partici;pate in these ongoing initiatives. CIP-01301 imposes too large a burden on roughly 1400 electric utilities within the bulk electric system.

Moreover, the Secretary of Energy has recently-granted (FAST Act) cyber security authority for the broader energy sector. Vulnerabilities of transmission and distribution utilities beyond FERC regulatory authority will foreseeably be channels through which foreign adversaries can attack the bulk electric system includng those portions that are subject to NERC-FERC standards. A broader framework is needed. The current draft Reliability Standard CIP-013-1 imposes substantial costs in time and money, and will not be a cost-effective initiative.

We respectfully urge NERC to provide fresh guidance to the Standard Drafting team to link proposed reliability requirements to broader initiatives, includng the Defense Science Board Report of February 2017 and findings of the Trump Administratioon as it reviews cyber strategy and policy initiatives.This standard will be wasteful of resources, and is not ready for prime time.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison

Answer	No
Document Name	

Comment

R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.

R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard

Implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.

Likes 0	
Dislikes 0	

Response

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1

Answer	No
Document Name	

Comment

Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Please refer to RSC- NPCC comments

Likes 0	
Dislikes 0	

Response

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4

Answer	No
Document Name	

Comment
Based on FE’s comments on the Requirements (R1-R5), review of the Implementation Plan is not relevant at this time.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3	
Answer	No
Document Name	

Comment
The implementation plan identifies that the effective date will be at least 12 months after the effective date of the applicable governmental authority’s order approving the standard or 12 months after the date the standard is adopted by the NERC Board of Trustees where approval by an applicable governmental authority is not required. Extending the initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 by as much as 15 months after the effective date of the standard seems to extend the improved supply chain risk management unnecessarily. PGAE believes the initial review and approval of the cyber security risk management plans specified in R2 should be completed on or before the effective date, so that subsequent Requests for Proposal and/or vendor contracts and applicable Service Level Agreements after the effective date can incorporate the R1 controls.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	

Comment
Since the effective date will be at least 12 months after NERC Board of Trustees approval under the current implementation plan, how does extending the initial review and update, as necessary, an additional 15 months provide for improved supply chain risk management? WECC believes the initial review and approval of the cyber security risk management plans specified in R2 should be completed on or before the effective date, so that subsequent Requests for Proposal [RFP] and/or vendor contracts and applicable SLAs after the effective date can incorporate the R1 controls.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. SRP requests a 24-month implementation plan.

SRP requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Response	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan.

CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	

We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Seminole does not believe that the standard is adequately defined to enable meaningful review of the implementation plan. Further, successful implementation of the plan is highly dependent on vendors and may require more than one year to implement.	
Likes 0	
Dislikes 0	
Response	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan.

CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan.

CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

Suggest breaking the implementation into three steps which follows CIP-014 – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline

The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities“ however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. AE requests a 24-month implementation plan.

AE requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment	
PRPA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. PRPA requests a 24-month implementation plan. PRPA requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan. CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Response	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	

ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
The implementation plan calls for R2 to be completed 15 months after the effective date of compliance of CIP-013; however, there is no requirement for signing the original R1 plan. Please clarify in R1 or R2 the required signature date for the supply chain cyber security plan.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy proposes an alternative Implementation Plan for the drafting team’s consideration. We agree with an Implementation Plan of 12 months for R1 and R2, and propose an Implementation Plan of 24 months for R3 and R4. We feel that based on the type of work and the workload that will be necessary to comply with R3 and R4 due to these requiring technical controls and configuration changes, a longer implementation plan is required.	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Suggest consider phasing the implementation of CIP-013 and CIP-003 Low BCS Physical, Electronic, TCA, and RM to reduce potential for resource constraints created by concurrent implementation of multiple programs.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities, “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification	
Likes 0	
Dislikes 0	
Response	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Response	

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Lack of a NERC definition of a PED makes it uncertain which products this (or any other) CIP standard applies-to. No new CIP standards should be developed until this issue is addressed. One year is not enough time, for the reasons stated above. A minimum of two years should be granted.	
Likes 0	
Dislikes 0	
Response	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item.	
Likes 0	
Dislikes 0	

Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	
12 calendar months may be inadequate if contracts are in the negotiation stage. 18 months may be more realistic; however, this is dependent on the language in the final set of requirements. We also recommend that the SDT consider how best to make it clear that this is a forward-looking standard as it relates to contracts, and the associated nuances. For instance, if you have a contract in place that allows for extensions or amendments, do you have to open up the entire contract when extending, making amendments, or minor revisions?	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item.	
Likes 0	

Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
Due to the early stage of development of this standard, NRECA is not able to support a specific Implementation Plan.	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
SVP agrees with other entities' comments to split the implementation plan into parts, e.g., identify risk, develop a plan and implement a timeline.	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI’s Position	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
The Implementation Plan is unfeasible as currently drafted. The proposed Standard should utilize a phased in implementation. In addition, the Standard and Implementation Plan do not address that CIP-013 only addresses new contractual obligations. This lack of clarity will likely cause issues during the enforcement period of the Standard.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
Oxy supports the comments of American Transmission Company, LLC	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Without being able to evaluate the Implementation Plan against the eventual final Standard, the company cannot offer its support.	
Likes 0	
Dislikes 0	
Response	

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
The technical controls required by R3/R4/R5 should be given additional time consideration. Perhaps 24 months to allow time to research and deploy technical controls of R3/R4/R5 while R1 – R2 are policy/contract-language driven only. Would a phased implementation approach be acceptable as a lot of the risks in R3, R4 and R5 have already been mitigated in CIP-007 and CIP-005 and therefore a maturity over time may make more sense?	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
The Standards as currently written require significant modifications to organizational procurement processes for big and small entities alike. Due to the scope of assets being considered, entities must implement central procurement in such a way for every cyber asset to filter through the rigorous process. The number of contracts cutting across BES and non-BES Cyber Systems are too numerous and complex to address as a separate CIP compliance process. This has the potential to require more organizational change than any of the previous version of CIP Cyber Security Standards. In comparison, CIP version 5 implementation allowed for 24 calendar months and fully resourced entities struggled to get the organizational processes	

perfected in time to meet the deadlines. We propose a minimum of 24 calendar months be allowed for the currently drafted Standard. We feel this is appropriate given the minimal time FERC has permitted for this Standard to be submitted.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra

Answer	No
Document Name	

Comment

1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

2) Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.

3) Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

4) Implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

The deferment of R2 by 15 months further supports the idea that the original documents do not have to be approved by the CIP Senior Manager, only subsequent revisions. The Implementation plan should at least require initial approval of the plans that are then subject to periodic review.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC disagrees with the implementation plan. The security controls identified will take significant time to implement, particularly as specified for low impact BES Cyber Systems. The suggestion of a 12 month implementation window implies that fundamentally the SDT does not appreciate the volume and diversity of low impact BES Cyber Systems across North America. Additionally, a 12 month implementation window does not allow time for entities to complete an annual budget cycle. As such, we strongly recommend that the SDT considers an 18 month implementation window at minimum. If any controls are kept for low impact, then a minimum 24 month implementation window should be provided for those controls.

Alternatively, GTC recommends the SDT to work with NERC to immediately begin to take the necessary actions to request more time from FERC to satisfy Order 829. This can be accomplished in 2 phases.

For the first phase, GTC believes the 12 month implementation window can be achieved if the SDT would limit the structure of CIP-013-1 to the supply chain context which ends at the delivery of products/services to the acquirer in accordance with NIST SP 800-53 r4 as outlined in GTC comments number 1 and 3.

For the second phase, GTC encourages for NERC to lay out a plan to FERC to better address the operational/technical requirements of R3 and R4 with the applicable existing CIP standards so that the correct technical experts can develop in a manner that would not create the double jeopardy scenarios described under the comments for R4 and R5. NERC could then request a 24 month window to address the operational technical requirements in the

correct applicable CIP standard. FERC provides NERC discretion per paragraph 44 the option of modifying existing Reliability Standards to satisfy the directive.

GTC recommends the SDT consider GTC's strategy in the comments above, and adapting the Implementation Plan accordingly.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Under initial performance, replace "of" with "following" so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…"

The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern.

We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification.

We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

The IRC and SWG are unclear how an entity will comply with requirements in R3, R4, and R5 if contracts have not been renegotiated to address the requirements with vendors. Further, clear criteria needs to be identified to determine when an entity must comply with the requirements. The applicability of the Standard should be clarified to address cyber assets procured prior to the CIP-013 effective date. Concerns to be considered include, (1) upon execution of a new agreement with the vendor, (2) upon installation of any new equipment, or (3) upon installation of any new software? Requiring compliance on new equipment or software will be problematic if the contractual agreements do not align.

The IRC and SWG request a 24-month implementation timeframe for CIP-013 R3 and R4 as budget cycle(s) will be required to support contractual issues, implementation, with possible automation of compliance evidence.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Under initial performance, replace “of” with “following” so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…”

The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern.

We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification.

We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment	
LCRA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. LCRA requests a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Response	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

Under initial performance, we recommend replacing “of” with “following” so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…”

The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern.

We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification.

We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. SMUD requests a 24-month implementation plan.

SMUD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	
The NYPA Comments	
Likes 0	
Dislikes 0	
Response	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Implementation plan must clearly state that all these requirements are forward looking and should not impact any existing contracts. We also believe that 12 months may not be enough to fully develop and implement a plan for large organizations to meet all four objectives. Perhaps a 24 month implementation period is appropriate. What is the difference between vendors, suppliers or other entities as stated in the implementation plan in the context of supply chain? None are defined terms.	
Likes 0	
Dislikes 0	
Response	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	

Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
Seattle City Light does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Seattle City Light requests a 24-month implementation plan. Seattle City Light requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The IESO suggest that in order to be consistent with the FERC Order that the standards be forward looking, clear criteria needs to be identified to determine when an entity must comply with the requirements. The applicability of the Standard should be clarified to address cyber assets procured prior to the CIP-013 effective date. Concerns to be considered include, (1) upon execution of a new agreement with the vendor, (2) upon installation of any new equipment, or (3) upon installation of any new software? Requiring compliance on new equipment or software will be problematic if the contractual agreements do not align.

The IESO request a 24-month implementation timeframe for CIP-013 R3 and R4 as budget cycle(s) will be required to support contractual issues, implementation, with possible automation of compliance evidence.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities

Answer	No
Document Name	

Comment

Colorado Springs Utilities (CSU) does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CSU requests a 24-month implementation plan.

CSU requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	No
Document Name	

Comment

Recommendation for a 24-month implementation process.

The implementation for the current CIP-013 standard is short. Many of the systems that are already in place under the current CIP standards were custom created or have features enabled to comply with the requirement(s) which they address. To comply with the standard requirements in CIP-013, in particular R4, registered entities may require modifications to the current processes and systems already in place or may require procurement of new components and/or services. The change process would require coordination with facility/equipment outages. A longer timeframe would be required for entities to effectively manage these changes without a negative impact to BES reliability. Also, to develop a supply chain risk management plan and implement that plan into our contracts would require more than 12 months to implement.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

2) Suggest breaking the implementation into three steps which follows CIP-014 – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline

3) The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities“ however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification.

Likes 0	

Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the lack of clear scope in the standard makes the evaluation of the implementation timeframe ambiguous. If the standard was adopted as written and required Low impact cyber asset inventories identification and evaluation, 24 months would be required to comply with the requirements.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. LCRA requests a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Santee Cooper does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Santee Cooper requests a 24-month implementation plan.	

Santee Cooper requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

In IPC's opinion, a 12 month effective date is not enough time to implement this standard given the amount of existing CIP standards currently in flux and new standards being developed. In addition, Regulatory guidance is often slow in coming, and entity budgetary cycles are usually at least 12 months. IPC suggests an 18–24 month effective date. An 18-month effective date is also consistent with the CIP-003-7 implementation plan.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation recommends that the implementation schedule be based on risk and enforced using a systematic approach. Under the systematic approach, Reclamation requests that plans affecting high impact BES Cyber Systems would be developed within 12 months of FERC approval, plans affecting medium impact BES Cyber Systems would be developed within 18 months of FERC approval, and plans affecting low impact BES Cyber Systems would be developed within 24 months of FERC approval.

Reclamation recommends that each plan should be implemented within 18 months of being developed.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
It is premature to accept/agree with any implementation plan due to the infancy of this proposed standard and potential risks, impacts, and unintended consequences that may ensue if the CIP-013-1 Standard were to move forward without adequately addressing the concerns of redundancy, lack of clarity, expansion in scope, or contradictory nature of the collective set of proposed requirements as described in above comments. Until the language can be improved so as not to create double jeopardy or an impossibly of non-compliance due to factors outside the control of the Registered Entity, or until a shift in approach can be agreed upon so as to leverage existing enforceable regulations that already provide the intended security or reliability benefit, ATC cannot support the proposed implementation plan.	
Likes 0	
Dislikes 0	
Response	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUC does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. OUC requests a 24-month implementation plan. OUC requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
We feel that the approval of the RSAW needs to be included in the documentation. This is another document that is pertinent to the Implementation Plan Process.	
Likes 0	
Dislikes 0	
Response	

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
The proposed 12-month implementation period and specification of an initial performance date for the CIP-013-1, R2 review and update appear reasonable. Texas RE requests the SDT provide a justification for the 12-month implementation period as part of the Standard development process.	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
In conjunction with the comments provided under R1 above, Southern Company supports the SDTs direction proposed in the Implementation Plan where it is applicable to the Supply Chain time horizon and industrial control system vendor products and services used in BES Cyber Systems, but requests the consideration of an 18 month (rather than 12 month) timeframe. For any requirements applicable to assets containing Low Impact BES Cyber Systems, given the volume and complexity of those assets, as well as the volume and diversity of agreements necessary between the Responsible Entity and it's suppliers of ICS products and services, Southern requests the consideration of a 24 month timeframe for implementation.	
Likes 0	
Dislikes 0	
Response	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wes Wingen - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
George Tatar - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	
Document Name	

Comment

Twelve months is not sufficient time to allow compliance with all aspects of this standard. The drafting team should consider a phased approach allowing the logical phased implementation of these requirements.

While the Implementation Plan suggests that existing contracts need not be modified, the proposed standard language does not make this clear. ERCOT believes the standard to be a more appropriate location for this exemption, as it is ultimately substantive in nature. ERCOT there recommends that the drafting team include language in the standard explicitly limiting applicability of the requirements to new contracts.	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

The VLS for R1

- The term "Either of the elements specified" in the Sever VLS is implying two elements when in fact I believe you are meaning "Any of the Elements in Either of the two requirement subparts."
- The High VLS specifies "…did not include one of the elements specified in Parts 1.1 or 1.2". Since one of these elements 1.2.7 is optional by inclusion of the "if applicable" language, this VSL should be rewritten to specifically exclude 1.2.7.

The VSL for R2

- Reviewing and modifying the plan reduce the risk, having a signature does not. Setting arbitrary times frames surrounding missing dates does not reduce risk. Recommend:
  - VSL lower - no signature
  - VSL Moderate - missing a new supply chain security risk during the review
  - VSL High - not performing review within 15 months
  - VSL Sever - not implementing needed control changes as identified from review

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Response	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

VSL for Requirement R3

Requirement R3 has four sub-parts which describe the software and firmware which need to be verified. ReliabilityFirst recommends the SDT structure the VSLs similar to Requirement 1 to address each of the sub-parts. ReliabilityFirst offers the following modifications for consideration

Lower VSL – The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify one of the elements specified in Parts 3.1 through 3.4.

Moderate VSL - The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify two of the elements specified in Parts 3.1 through 3.4.

High VLS – The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify three of the elements specified in Parts 3.1 through 3.4.

Severe VSL - The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.

VSL for Requirement R5

To account for instances where the Responsible Entity had cyber security policies specified in the requirement but were not reviewed for 18 months or greater, ReliabilityFirst recommends the following “OR” statement be added to the Severe VSL Category:

Additional Severe VLS - The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 18 calendar months from the previous review.

Likes 0

Dislikes 0	
Response	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Response	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI does not agree with the requirements as written and accordingly cannot agree with the proposed VRFs and VSLs proposed for those requirements in CIP-013-1.	
Likes 0	
Dislikes 0	
Response	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	
Response	

Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	

PRPA does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, PRPA requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. PRPA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Response	

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	
AE does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, AE requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. AE requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	

For R3 and R4: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

Do not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No
Document Name	

Comment

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	No
Document Name	

Comment

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	

Comment

Seminole does not believe that the standard is adequately defined to enable meaningful review of the VRF and VSL.

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	
Comment	
CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
Response	

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	
SRP does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, SRP requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.	

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. SRP requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

WECC believes missing one of the elements of Part 1.2 in the VSL for Requirement R1 should be considered lower risk than missing one of the elements in Part 1.1, as it seems to be a subset of Part 1.1., and should be assessed at moderate risk. WECC agrees that missing one of the elements of Part 1.1 is appropriately identified as a High VSL.

In the VSL for Requirement R5 there is no language for a Responsible Entity that had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, but the approval was more than 18 calendar months from the previous review. WECC believes a third entry should be added to the Severe VSL for Requirement that reads:

The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however, the approval was more than 18 calendar months from the previous review.

Additionally, in the high and severe VSL language of R5 it appears that the word "but" before the words "did not include" should be deleted.

Likes 0	
Dislikes 0	

Response

John Hagen - Pacific Gas and Electric Company - 3

Answer	No
Document Name	

Comment

PGAE believes missing one of the elements of Part 1.2 in the VSL for Requirement R1 should be considered lower risk than missing one of the elements in Part 1.1, as it seems to be a subset of Part 1.1., and should be assessed at moderate risk. We agree that missing one of the elements of Part 1.1 is appropriately identified as a High VSL.

Likes 0	

Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	
Based on FE’s comments on the Requirements (R1-R5), review of the VRFs and VSLs is not relevant at this time.	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Response	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
We have not reviewed with care, but consider the standard requirements need fundamental reworking before addressing VRFs and VSLs.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
There is a concern that there is an inconsistency with the risk impact classification for the Requirements, and VSLs. We feel that these inconsistencies have the potential to lead to Compliance Enforcement issues in reference to the proper alignment of both sections. For example, the VSLs for Requirement R3 and Requirement R4 focus on high and medium, however, Requirement R5 mentions low impact. We feel that all three (3) classifications need to be considered in all of the Requirements language to have a successful Standard.	
Likes 0	
Dislikes 0	
Response	
Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	
The VRFs and VSLs will need to be incorporated in CIP-002 through -011 where changes are made.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	

Comment

- We recommend that requirements R1 and R2 should be low based on the fact the requirements are administrative in nature (i.e., deal with the procurement), and if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the Emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System.
- We recommend that requirement R5 should be Low because it is related to CIP-003-6 which is also Low.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	

Comment

Due to our concerns expressed in this document, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	
Dislikes 0	

Response

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	

Comment

There is a concern that there is an inconsistency with what is stated in the Requirements, VRFs, and VSLs. These inconsistencies have the potential to lead to Compliance Enforcement issues in reference to those particular elements of the Standard and therefore, NRG recommends alignment between

Requirements, VRFs, and VSLs. NRG suggests that this language be properly aligned with the requirements (recommendation for Low or Moderate VSLs relating to process controls) or else this could lead to future Compliance Enforcement issues for the industry.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	No
Document Name	

Comment

Same as RoLynda Shumpert's comments from SCE&G:

Due to our concerns expressed in this document, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	
1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL. 2) For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted. 3) For R4: See comment above for R3.	
Likes 0	
Dislikes 0	

Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The VRFs and VSLs seem harsh. CenterPoint Energy does not agree with the automatic High VSL for any element not fully addressed, in a Regional Entity's opinion, by a Responsible Entity's risk management plan, especially given the extremely vague bounds presented on what represents a valid risk management methodology, planning process, evaluation method, or mitigation effectiveness measure.	
Likes 0	
Dislikes 0	
Response	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Response	
Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUCX does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, OUC requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. OUC requests considering all of the nine sub-requirements of	

R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
It is premature to accept/agree with the VRFs or VSLs due to the infancy of this proposed standard and potential risks, impacts, and unintended consequences that may ensue if the CIP-013-1 Standard were to move forward without adequately addressing the concerns of redundancy, lack of clarity, expansion in scope, or contradictory nature of the collective set of proposed requirements as described in above comments. Until the language can be improved so as not to create double jeopardy or an impossibly of non-compliance due to factors outside the control of the Registered Entity, or until a shift in approach can be agreed upon so as to leverage existing enforceable regulations that already provide the intended security or reliability benefit, ATC cannot support the proposed VSLs/VRFs.	
Likes 0	
Dislikes 0	
Response	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	

Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
The sub-requirements within each requirement should be used to distinguish the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	
IPC feels all VSLs should be set to low the first year of enforcement and then increase the VSL after year one of enforcement. This allows for process refinement without significant penalty.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Santee Cooper suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Santee Cooper suggests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and constructs the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. LCRA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA suggests the VRFs and VSLs include consideration for instances where the vendor or supplier is not able or is unwilling to support the standard requirement.

Likes 0	

Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	

Comment
1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL. 2) For R3 and R4: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted. 3) Do not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	

Comment
CPS Energy supports the comments provided by APPA

Likes 0	
Dislikes 0	

Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	

Colorado Springs Utilities (CSU) does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CSU requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CSU requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The IESO requests review to ensure violations align with impact ratings and existing standards program.

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, policies and plans are implemented while processes are performed. If a policy or plan is required to be implemented and there is an instance where a process included as part of the policy or plan, is not adhered to, then this would result in a violation of the policy or plan but not in the requirement to implement the policy or plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not

followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted

For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	

Comment

Seattle City Light does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Seattle City Light requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Seattle City Light requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3

Answer	No
Document Name	

Comment

FEUS supports the comments submitted by APPA

Likes 0	
Dislikes 0	

Response
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment
FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response
Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment
The NYPA Comments

Likes 0	
Dislikes 0	

Response
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, SMUD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. SMUD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. LCRA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	

Comment

The IRC and SWG requests review to ensure violations align with impact ratings and existing standards program.

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, policies and plans are implemented while processes are performed. If a policy or plan is required to be implemented and there is an instance where a process included as part of the policy or plan, is not adhered to, then this would result in a violation of the policy or plan but not in the requirement to implement the policy or plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted

For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	

Comment

Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.

Likes 0	

Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC recommends the SDT consider GTC's comments above, and adapting the VRFs and VSLs accordingly.	
Likes 0	
Dislikes 0	
Response	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The VRF mapping based on the ERO Final Blackout Report is questionable because CIP-013 only addresses the possible inclusion of non-authentic or compromised hardware, firmware, and software; and does not speak to the risk level of the inclusion. The same compromised hardware, software, or firmware will pose different risks to the BES based upon the inherent risk to the BES by the Entity. The VSL's are acceptable from a documentation administration standpoint, but do not correspondinly map to the impact resulting. While it is now appropriate to be generating ideas on VRF and VSL for CIP-013, a final determination should wait until the industry is closer to consensus on the actual requirements.	
Likes 0	
Dislikes 0	
Response	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	

Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	

Comment
Requirement R2 calls for the periodic review of existing plans and approval of updates. This is mostly a documentation management requirement and the VRF could be defined as Lower instead of Medium. Compromised software integrity is a key element of previous successful cyberattacks, including Havex. The VRF for Requirement R5 needs to be Medium even though the focus of the Requirement is on Low Impact BES Cyber Systems. The Severe VSL for Requirement R1 should refer to failing to include two or more elements of Parts 1.1 or R1.2. While that should be able to be presumed from the lesser applicability of the High VSL for R1, it is not sufficiently clear.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	

Comment
Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	

Comment
1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements

of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

2) For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

3) For R4: See comment above for R3.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	No
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment

The VRF mapping based on the Final Blackout Report is questionable because CIP-013 only addresses the possible inclusion of non-authentic or compromised hardware, firmware, and software; and does not speak to the risk level of the inclusion. The same compromised hardware, software, or firmware will pose different risks to the BES based upon the inherent risk to the BES by the Entity. The VSL's are acceptable from a documentation

administrative standpoint, but do not map to the risk presented. While appropriate to be generating ideas on VRF and VSL, final determination should wait until the industry is closer to consensus on the actual requirements.	
Likes 0	
Dislikes 0	
Response	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Response	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Without being able to evaluate the VRFs and VSLs against the eventual final Standard, the company cannot offer its support.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	

Oxy does not agree with the proposed language of the requirements and therefore cannot agree with the VRF's and VSL's until requirements are revised and updated and corresponding updates are made to the VRF's and VSL's.

Likes 0	
Dislikes 0	

Response

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Concur with EEI's Position

Likes 0	
Dislikes 0	

Response

Val Ridad - Silicon Valley Power - 1 - WECC

Answer	No
Document Name	

Comment

-- See comments from APPA, with which SVP agrees.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No
Document Name	

Comment

Due to the early stage of development of this standard, NRECA is not able to support a specific set of VRFs and VSLs.

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	

For R5, the mention of part 5.1 should be removed for High and Critical (see comments on R5 above).

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

No Comments

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	Yes
Document Name	

Comment

We agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), provided that they should be updated to reflect changes to the proposed Standards Requirements consistent with the recommendations discussed in questions 1-6.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

In light of all previous comments made above, Southern Company requests that the SDT also consider the VSLs for R3, which should accommodate other levels of severity with regard to verifying integrity and authenticity of industrial control system vendor products, software, patches, and/or upgrades. As currently written, any violation of R3 is considered Severe. There are more granular levels of severity to be considered, for example – when a Responsible Entity has a plan(s), has implemented that plan(s), but a percentage of a volume of patches applicable to a particular business unit (out of many business units within a Responsible Entity) were not adequately validated.

Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF

Answer	
Document Name	

Comment

N/A

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response
Kenya Streeter - Edison International - Southern California Edison Company - 6
Answer	
Document Name	
Comment
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison
Likes 0	
Dislikes 0	
Response
Fred Frederick - Southern Indiana Gas and Electric Co. - 3
Answer	
Document Name	
Comment
No comment
Likes 0	
Dislikes 0	
Response
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1
Answer	
Document Name	
Comment
Vectren does not vote in non-binding polls. (VRFs and VSLs).
Likes 0	
Dislikes 0	
Response

Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	
These will be reviewed in-depth after changes are made to the requirements.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Response	

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The Technical Guidance and Examples makes it more evident as to how much of CIP-013 is duplicative of exisiting CIP Standards. CenterPoint Energy strongly recommends that the CIP-013 draft be edited as noted and the Technical Guidance and Examples be revised accordingly.	
Likes 0	
Dislikes 0	
Response	

Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	
1) The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.	

2) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

3) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

4) Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

5) Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

6) Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

7) Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

8) Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

9) Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

10) Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

11) Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

12) Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

13) Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

1) Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

2) Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

3) Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

4) Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

5) Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

6) Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

7) Page 11, Line 15, replace supplier with Vendor.

8) Page 11, line 25, replace “should” with “may”

9) Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

10) Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

11) Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

12) Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

13) Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	No
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	

Same as RoLynda Shumpert's comments from SCE&G:

Although the Guidelines and Technical Basis document has been helpful, it will need further changes to reflect the changes in the requirements driven by concerns of Regional Entities.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Page 16 line 25, replace “should” with “may”.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Although the Guidelines and Technical Basis document has been helpful, it will need further changes to reflect the changes in the requirements driven by concerns of Regional Entities.	
Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Recommend removing the responsible entities section in this document as the entities are already outlined in the Standard itself.
- Page 1 Line 42: additional language should be added to address existing contract extensions or addendums, effectively excluding them as well.
- Recommend revising this document based on the revisions made to CIP-013.

Likes 0	
Dislikes 0	
Response	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	
Comment	

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

CIP-002 through -011 Guidelines and Technical Basis should be updated to reflect revisions to those standards and to ensure there is not conflicting guidance.

Outside of the Guidelines and Technical Basis in the standards, other implementation guidance could be proposed for the ERO deference process.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	No
Document Name	

Comment

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 – Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – Same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins

Answer	No
Document Name	

Comment

Technical Guidance and Examples

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

We feel that there is inconsistency with the language of the Requirements and The Technical Guidance language specifically in reference to Requirement R3 and Requirement R4. The guidance section for both Requirements mentions reviewing security policies. However, the Requirements mention Risk Management Plans. We feel that this language needs to be properly aligned or this will lead to future Compliance Enforcement issues for the industry.

Likes 0	
Dislikes 0	

Response

OSI Open Systems International - OSI Open Systems International - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

As a vendor of SCADA/EMS/TMS systems for many NERC Responsible Entities, OSI (Open Systems International Inc.) is providing the following comments to the NERC CIP-013 SDT for consideration. All suggested text additions are identified in ***bold-italics*** font.

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services;

OSI recommends that the SDT consider an additional comment for paragraph 5 as follows:

Personnel background and screening practices by vendors. ***Note that state & local laws may prevent vendors from sharing certain private information about their employees as related to their background screening (eg. social security numbers).***

OSI recommends that the SDT consider an additional comment for paragraph 9 as follows:

System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout their processes. ***Vendor policies showing adherence to appropriate industry standards for secure development processes is an acceptable method for Responsible Entities to demonstrate due diligence. An example of acceptable industry standards for secure development are the various System & Services Acquisition (SA) controls related to SDLC within NIST 800-161.***

Note that NIST 800-161 is the standard used by U.S. Government entities to ensure Supply Chain Security for all departments and sites.

OSI recommends that the SDT consider an additional comment for paragraph 10 as follows:

Review of certifications and their alignment with recognized industry and regulatory controls. ***It is important that Responsible Entities consider which industry certifications are applicable for each vendor's line of business and not use a "one size fits all" approach. For example, NIST 800-161, ISO-27001 are relevant standards pertaining to computer system security. On the other hand, inclusion of requirements for non-relevant or specialized certifications could disqualify certain vendors (eg. certifications used by the financial industry).***

R1.2 Potential Procurement Controls

It is OSI's opinion that the current CIP-013 non-prescriptive approach to the development of procurement controls will lead to an unsustainable permutation of controls and associated contracts for vendors supporting the industry. The extreme diversity of procurement controls/contracts may push certain vendors away from the bidding process, ultimately reducing competition and increasing costs for the industry as a whole. OSI strongly urges that NERC and the CIP-013 SDT consider the addition of acceptable examples of compliance for different classifications of industry vendors eg. SCADA software vendors, RTU vendors, transformer vendors, etc. NERC and Regional Entity endorsement of such examples will provide both vendors and entities with a sensible baseline for procurement controls. OSI is providing an example of guidance for SCADA/EMS vendors as follows:

The following represents example procurement controls that can be considered for EMS/TMS/SCADA system vendors. This set of controls is not the only method of achieving compliance, but it is considered by NERC to be one acceptable method.

The following "National Institute of Standards and Technology" (NIST) standards can be used to satisfy R1.2. Controls that are applicable to the EMS/TMS/SCADA vendor should be extracted from the various sections to utilize within a procurement contract for compliance with R1.2.

- ***NIST 800-161: "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"***
- ***AC – Access Controls***

- ***AT – Security Awareness and Training***
- ***AU – Audit and Accountability***
- ***CA - Security Assessment and Authorization***
- ***CM – Configuration Management***
- ***CP – Contingency Planning***
- ***IA – Identification and Authentication***
- ***IR – Incident Response***
- ***MP – Media Protection***
- ***PE – Physical and Environmental Protection***
- ***PL – Security Planning***
- ***PM – Security Program Management***
- ***PS – Personnel Security***
- ***PV – Provenance***
- ***RA – Risk Assessment***
- ***SA – System and Services Acquisition***
- ***SC – System and Communications Protection***
- ***SI - System and Information Integrity***
- ***NIST 800-82 "Guide to Industrial Control Systems (ICS) Security***

R1.2.3 Processes for disclosure of known vulnerabilities:

The guidance document currently states the following: "*Request vendor cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed."*

Vendor release of information concerning **uncorrected** non-public vulnerabilities represents a security threat for the entire industry and is contrary to best practices in the software industry and most vendor's security policies. When a vendor provides such information to a single Responsible Entity, the entire industry is placed at further risk of the information being publically released without a mitigation. There are many industry documents on this topic and as an example OSI strongly urges that SDT review the "Vulnerability Disclosure Framework" documented on the DHS website from the National Infrastructure Advisory Council at the following link:

https://www.dhs.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf

The DHS publication states the following as part of its overall recommendations to the President:

"Protect the confidentiality of vulnerabilities for which no known exploitations have been reported while affected vendors are working towards a solution. Coordinate the voluntary disclosure of information regarding exploited vulnerabilities to take into account, among other factors, the risks of damage to the nation's critical infrastructure, the need for completion of ongoing investigations, and the coordinated release of solutions or remedies for the vulnerability."

Some Responsible Entities may believe that they can protect such critical information, but the reality is that their protection is only as strong as their weakest employee clicking on a phishing link. When you consider releasing uncorrected or unmitigated vulnerability details to multiple Responsible Entities of all sizes and levels of security training, the risk of that information falling into the hands of bad actors becomes very high.

OSI therefore strongly urges NERC and the CIP-013 SDT to remove the word "**uncorrected**" from the guidance statement. OSI believes it is critically important to utilize language that does not attempt to compel or otherwise recommend that Responsible Entities request disclosure of uncorrected or unmitigated vulnerabilities from any vendor. OSI will not agree to provide such information and most other vendors will likely adopt the same position. On the other hand, vendors that do agree to these provisions and the entities receiving such information are placing the entire industry at further risk until a mitigation is made available by the vendor – which could be weeks or months after bad actors become aware of the vulnerability. Responsible vendors will not disclose uncorrected vulnerabilities but will provide recommended mitigations if they are available.

R1.2.5 Processes for verifying software integrity and authenticity of all software and patches that are intended for use:

OSI recommends additional wording in the final paragraph as follows:

When third-party components are provided by the vendor, request vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses ***within a reasonable period that enables the vendor to integrate and complete certification testing of the updated third-party component.***

R1.2.6 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

OSI recommends additional wording in the 3rd paragraph as follows:

Request vendors maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity. ***The vendor's use of a proxy or intermediate host to provide isolation of connections to Responsible Entity's equipment is one example of best practices for remote access.***

R1.2.7 Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable

OSI recommends additional wording in the 1st paragraph as follows:

Request vendors provide Responsible Entity with audit rights that allow the Responsible Entity or designee to audit vendor's security controls, development and manufacturing controls, access to certifications and audit reports, and other relevant information. ***Responsible Entity review of vendor audit reports completed by industry recognized certification groups can be used as an acceptable method to verify a vendor's security posture. Examples are certified auditor reports for ISO-27001, NIST, etc.***

R4 Part 4.1 Potential Remote Access Controls

Based on the NERC Lessons Learned document at this link (http://www.nerc.com/pa/CI/tpv5impmntnstdy/Vendor%20Access%20Management%20Lesson%20Learned.pdf) , OSI recommends additional wording as follows:

One acceptable example of best practice is to use a process whereby the remote access session is initiated by the Responsible Entity, and the token code is provided verbally from the Entity to the vendor when requested by the authentication system. This method ensures that the Responsible Entity is in control of the session and the vendor is not allowed access without knowledge of the Entity.

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Response	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	
Comment	

The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan.

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple places in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Page 16 line 25, replace “should” with “may”.

The Implementation Plan should more clearly state that contract renegotiation is not necessary during the implementation period if a contract has already begun.

“Vendor” should be a defined term. The Standard should have consistent use of the terms, i.e., only use “vendor” and do not say “third-party.”

Are sub-component manufacturers included under the term “vendor”?

Likes 0	
Dislikes 0	
Response	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	
Comment	
Too many changes to the standard to adequately comment on the *Technical Guidance and Examples* document.	
Likes 0	
Dislikes 0	
Response	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	
Based on FE's comments on the Requirements (R1-R5), a detailed review of the Technical Guidance and Examples document is not relevant at this time. However, FE suggests that, in general, it would be helpful if the Technical Guidance and Examples document could provide evidence formats, similar to what is provided in CIP-003-6 Attachment 2.	
Likes 0	

Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

SRP requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

SRP requests clarification on the term “supplier” as it is used in the guidance document. SRP requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, SRP requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. SRP requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced SRP requests that the SDT define the term and place it in the NERC Glossary of Terms.

SRP requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. SRP requests that the following language be added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, SRP requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment

We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	No
Document Name	
Comment	

Portions of the *Technical Guidance and Examples* document that may affect how the standard is interpreted for audit purposes should be placed in the standard's Guidelines and Technical Basis section and needs to be balloted and approved by industry. As this is not a part of the standard and is not a CMEP Practices Guide, this document should provide implementation guidance in a manner consistent with the NERC Compliance Guidance Policy "to develop examples or approaches to illustrate how registered entities could comply with a standard that are vetted by industry and endorsed by the ERO Enterprise." The implementation guidance is an important item for this standard and Seminole appreciates this work.

As implementation guidance, this document should provide a clear standard manner to address requirements for R1.1 and R1.2.1-R1.2.6, while entities may be able to ask additional questions. While the document discusses ideas of what to include, the biggest value would be to provide an example set of specific questions to vendors on risk management controls. By setting this specification up front, costs drop for both vendors and entities as the vendors can provide the basic set of information in a defined format. Once vendors have a better defined set of expectations, they then know how to meet these expectations across the industry, Further, vendors focused on the electric sector will provide this information, as we are their market. However, we all also use smaller software and hardware vendors that primarily service a broader market, and these smaller vendors would be less willing to provide custom information for separate electric sector entities for a sale amounting to tens or hundreds of dollars.

Open source software does not have a cost or a defined vendor. Risk assessment of open source software should be specifically addressed.

As there is no consistency in the software industry on use of hash functions, guidelines need to be provided on what is considered an acceptable approach to meet this requirement.

This standard essentially eliminates the ability to purchase equipment or services on an emergency basis without a pre-existing contract. This will interfere with incident response and BES recovery operations under extraordinary circumstances.

Likes 0	
Dislikes 0	
Response	

W. Dwayne Preston - Austin Energy - 3

Answer	No
Document Name	
Comment	

I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	
Response	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

AE requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

AE requests clarification on the term “supplier” as it is used in the guidance document. AE requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, AE requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. AE requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced AE requests that the SDT define the term and place it in the NERC Glossary of Terms.

AE requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. AE requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, AE requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	No
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment

PRPA requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

PRPA requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

PRPA requests clarification on the term “supplier” as it is used in the guidance document. PRPA requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, PRPA requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. PRPA requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced PRPA requests that the SDT define the term and place it in the NERC Glossary of Terms.

PRPA requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. PRPA requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, PRPA requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5

Answer	No

Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
As the SDT addresses the comments above regarding the standards, we assume the Technical Guidance and Examples will be modified accordingly.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The Guidelines and Technical Basis should include examples to illustrate how implementation is envisioned, and how entities are to be expected to coordinate between SME's and procurement organization, which up to now has not been engaged directly in NERC CIP implementation.	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

More focus should be given to implementation as opposed to justification. I think we all agree with respect to the importance of making sure the Supply Chain is free of malware and although some justification may be necessary to further explain the merits of adding a few additional requirements to the process, overall we are more concerned with implementation strategy. Those implementation methods would better serve us in our own internal controls and for evidence preparation in order to meet the compliance objectives.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott; Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	No
Document Name	

Comment

AEP is concerned about the use of the term “should” in the *Technical Guidance and Examples* document. While AEP understands that the intent of this document is to provide guidance and examples, the use of term “should” may be interpreted by the regional auditors as closer to a mandatory requirement. In order to address this concern, the document could use the term “may” instead. AEP is concerned that this is a shift away from traditional guidelines and technical basis documents, which documents the drafting team’s considerations. The proscriptive nature of this document is concerning when left to the interpretation of different auditors. AEP would not want this document to become akin to an actual Requirement without going through the proper process.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	No
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	

The statement on p.1 that CIP-013-1, “does not require the Responsible Entity to renegotiate or abrogate existing contracts,” implies that no action needs to be taken for existing PEDs. This point should be made explicit in the standard per se, but our “additional comments” concerns would still apply for replacing or upgrading existing equipment.

The Technical Guidance and Examples document should be revised to address our negative-ballot comments. Our concerns regarding willingness and ability of vendors to be CIP-013-friendly appear to already be at least partly recognized, ref. for example the statement on p.3, “Obtaining the desired specific cyber security controls in the negotiated contract may not be feasible with each vendor.” The subsequent comment that “every negotiated contract will be different,” indicates however that we and the SDT are not on common ground regarding practicality.

Likes 0	
Dislikes 0	
Response	

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	

The standard as written doesn’t clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

Although NERC’s Compliance Guidance Policy document describes certain procedures by which a drafting team may provide Compliance Guidance, ERCOT suggests that it is generally preferable to provide examples of acceptable conduct in the standard itself, rather than in an ancillary document, which Responsible Entities would have to remember and separately locate and review. The team could achieve this purpose by using language in the standard such as: “Practices that comply with this requirement include, without limitation, the following: . . . .” ERCOT notes that in a number of

instances, the draft Technical Guidance and Examples document uses normative language (e.g., “should”), rather than permissive (e.g., “may”) language, which suggests that the Technical Guidance document is instead intended to serve simply as a more detailed set of requirements, as opposed to describing one of potentially many acceptable methods of achieving compliance. For example, the guidance for R1 states: “In implementing Requirement R1, the responsible entity should consider the following: . . . .” To the extent the drafting team intends the guidance in this document to be followed, it should be included in the standard.

Likes 0	
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	No
Document Name	

Comment

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.

Likes 0	
Dislikes 0	

Response

Luis Rodriguez - El Paso Electric Company - 6

Answer	No
Document Name	

Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
Due to the early stage of development of this standard, NRECA is not able to support specific Technical Guidance and Examples.	
Likes 0	
Dislikes 0	
Response	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	

Oxy does not agree with the proposed language of the requirements and therefore cannot agree with the *Technical Guidance and Examples* document until requirements are revised and updated and corresponding updates are made to the *Technical Guidance and Examples* document.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	No
Document Name	

Comment

Without being able to evaluate the Technical Guidance and Examples document against the eventual final Standard, the company cannot offer its support.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	No
Document Name	

Comment

We generally agree with EEI’s comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	No
Document Name	

Comment
The Technical Guidance Document is well-written based upon what the NERC Drafting Team had to work with, but the controls recommendations are expansive enough to become its own industry. This would be an excellent document to use as a starting point of conversation with our hardware and software supply chain, but to impose it on the Entities as the end customers of these ICS products and applications would be overly burdensome with very little return on investment. This would be particularly true for those Entities dealing only with Low Impact BCS.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	

Comment
See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	

Comment
1) The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”. 2) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two. 3) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

4) Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

5) Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

6) Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

7) Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

8) Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

9) Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

10) Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

11) Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

12) Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

13) Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

14) Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service

acquisition and implementation". It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting "and/or operational phase of".

15) Page 6, line 1. Provide explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

16) Page 6., line 5. Notification of all "identified, threatened attempt" is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor's security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

17) Page 6, line 6: Is the ("Security Event") being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that "have potential adverse impacts to the availability or reliability of BES Cyber Systems" be part of the definition.

18) Page 6, line 22: For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given. Request clarification as to how this guidance for "requested cooperation" would meet the required "notification".

19) Page 9 lines 6 and 8: correct numbers "2.2" and "2.3" to be "2.1" and "2.2".

20) Page 11, Line 15, replace supplier with Vendor.

21) Page 11, line 25, replace "should" with "may"

22) Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

23) Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

24) Page 12 line 33. Provide additional clarity on "monitor". Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

25) Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

26) Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

27) Page 16 line 25, replace “should” with “may”.

Likes 0	
Dislikes 0	

Response

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick

Answer	No
Document Name	

Comment

Avista supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment

Requirement R1 needs to be vendor focused. It is not appropriate to assign risk based on the categorization of BES Cyber System impacted by the procurement. This Standard is for supply chain management, not BES Cyber System management. The guidance should not be limited to a brief discussion of Black Energy. To the contrary, the risks presented by Havex appear to be the stronger driver of need as perceived by FERC. It is imperative that vendor risk management controls, such as those cited on Page 4, starting at Line 13, comport with the substantively same or similar requirements of other CIP Standards before being allowed. The Guidance should also address the situation where the Registered Entity has chosen a patch source, per CIP-007-6, Requirement R2, that is not the originator of the software. For example, where the Registered Entity chooses to get its Microsoft and Linux patches from its SCADA/EMS vendor. Some sort of integrity chain needs to be verified.

Likes 0	
Dislikes 0	

Response
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich

Answer	No
Document Name	

Comment
See comments submitted by Black Hills Corporation

Likes 0	
Dislikes 0	

Response
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment
The Technical Guidance Document is well-written based upon what the NERC Drafting Team had to work with, but the controls recommendations within this document are expansive enough to become its own industry. This would be an excellent document to use as a starting point of conversation with our hardware and software supply chain, but to impose it on the Entities as the end customers of these ICS products and applications would be overly burdensome with very little return on investment. This would be particularly true for those Entities dealing only with Low Impact BCS.

Likes 0	
Dislikes 0	

Response
Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment
GTC recommends the SDT consider GTC’s comments above, and adapting the Technical Guidance and Examples document accordingly.

Likes 0	
Dislikes 0	

Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	
R1: The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an existing contract? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard or in the implementation plan. Please clarify how existing versus new procurement elements are addressed, especially for R3 and R4 technical controls.	
Likes 0	
Dislikes 0	
Response	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

As the *Technical Guidance and Examples* is not legally enforceable LCRA cannot rely on it as an authoritative source for guidance on complying with CIP-013.

Likes 0	
Dislikes 0	

Response

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	

Comment

SDG&E agrees with EEI comments and proposed language.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	No
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

SMUD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

SMUD requests clarification on the term “supplier” as it is used in the guidance document. SMUD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, SMUD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. SMUD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced SMUD requests that the SDT define the term and place it in the NERC Glossary of Terms.

SMUD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. SMUD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, SMUD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	

Comment

The NYPA Comments

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	No
Document Name	

Comment

FMPA agrees with comments submitted by American Public Power Association.

Likes 0	

Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	

Comment
FEUS supports the comments submitted by APPA

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	

Comment
Seattle City Light requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging. Seattle City Light requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. Seattle City Light requests clarification on the term “supplier” as it is used in the guidance document. Seattle City Light requests replacing with the term vendor or providing clarification on the difference between the two. In the guidance document on page 6, line 1, Seattle City Light requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.” The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. Seattle City Light requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced Seattle City Light requests that the SDT define the term and place it in the NERC Glossary of Terms. Seattle City Light requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. Seattle City Light requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities. Additionally, Seattle City Light requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	

Dislikes 0	

Response

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	

Comment
R1: The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an existing contract? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard or in the implementation plan. Please clarify how existing versus new procurement elements are addressed, especially for R3 and R4 technical controls.

Likes 0	
Dislikes 0	

Response

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	

Comment
CSU requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging. CSU requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. CSU requests clarification on the term “supplier” as it is used in the guidance document. CSU requests replacing with the term vendor or providing clarification on the difference between the two. In the guidance document on page 6, line 1, CSU requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CSU requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CSU requests that the SDT define the term and place it in the NERC Glossary of Terms.

Colorado Springs Utilities (CSU) requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CSU requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CSU requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Nathan Mitchell - American Public Power Association - 3,4

Answer	No
Document Name	

Comment

1) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

2) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or, define the term.

3) Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

4) Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be either defined in this standard or in the NERC Glossary of Terms. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition. The “threatened, attempted” part of this definition would is too large in scope and could require large vendors like Microsoft or Cisco to report thousands or millions of attempts each day. Suggest replacing “vendor security event” in R1.2.1 with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

5) Page 6, line 12: It is unclear that the R1.2.1 requires notification by the entity to the vendor.

6) Suggest adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

7) In other standards, the Guidelines and Technical Basis document is included in the standard, suggest that this also be completed for CIP-013.

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA proposes the “Supply Chain” requirements should be clear on what is to be done during the procurement process. Any aspects of service or ongoing maintenance activities should be addressed in the appropriate CIP standard. All requirements for Low impact systems should be in CIP-003.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	No
Document Name	

Comment

As the *Technical Guidance and Examples* is not legally enforceable, LCRA cannot rely on it as an authoritative source for guidance on complying with CIP-013.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper suggests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging.

Santee Cooper requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

Santee Cooper requests clarification on the term “supplier” as it is used in the guidance document. Santee Cooper suggest using consistent terms between the standard and the Technical Guidance.

In the guidance document on page 6, line 1, Santee Cooper requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. Santee Cooper requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset.

Additionally, Santee Cooper requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

The Technical Guidance and Example language states, “Entity processes for addressing software risks and vendor remote access risks per Requirements R3 and R4. Consider whether to include low impact BES Cyber Systems in these processes, or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber Systems.” R5 states that Responsible Entities must have “one or more documented cyber security policies.” IPC would like to know why the Technical Guidance and Examples language directs Responsible Entities to consider developing “processes” to meet a requirement that explicitly states that Responsible Entities must have “one or more documents cyber security policies” to meet the requirement?

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

The entire standard addresses supply chain risk management and therefore should address the possible risks and possible controls for entities to consider for each stage of the life cycle of a system in which there is interaction with and dependence on vendors, their products, and/or their services. These may include but are not limited to evaluation of design, procurement, acquisition, testing, deployment, operation, and maintenance. Reclamation recommends the technical guidance document provide examples of risks and their respective controls (such as contract clauses) for entities to consider.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	No
Document Name	

Comment

1. Please include guidance on expectations for resource and time to support the requirements. Most low impact entities do not have a procurement office or manager and are wondering who should be hired or trained to support the supply chain issues.

Likes 0	
Dislikes 0	

Response

Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli

Answer	No
Document Name	

Comment

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).

Likes 0	
Dislikes 0	

Response

Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
This document identifies some shortcomings, pitfalls, and/or unintended consequences of prescribing requirements within a mandatory reliability standard and is evidence that a Reliability Standard may not be the best vehicle to address the complexities and broad range of individual Registered Entity nuances in process and infrastructure, on top of the host of jurisdictional, technical, economic, and business relationship issues associated to supply chain; and further demonstrates the essentiality of reconsidering the need for CIP-013-1.	
Likes 0	
Dislikes 0	
Response	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUC requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging. OUC requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. OUC requests clarification on the term “supplier” as it is used in the guidance document. OUC requests replacing with the term vendor or providing clarification on the difference between the two.	

In the guidance document on page 6, line 1, OUC requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. OUC requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced OUC requests that the SDT define the term and place it in the NERC Glossary of Terms.

OUC requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. OUC requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, OUC requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Response

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

(Page 2, lines 2-3) An entity should define its specific approach to the SCRM plan in the preamble, so the Regional Entity will be able to evaluate the development and application of the plan.

(Page 2, lines 16-24: This passage gives entities a huge pass on implementation. As long as the entity asked the vendor to play nice during the RFP process, it appears the entity may not be found in noncomoliance if the final vendor contract does not include part or all of the entity's SCRM RFP clauses. This means it will be important to evaluate both the RFP and the final Service Level Agreement [SLA]/Contract for a specific applicable BCS. This review may lead to Recommendations and/or Areas of Concern [AoC], but might be difficult to substantiate Possible Non-Compliance [PNC] Finding as long as the RFP process aligns with the entity's SCRM plan.

(Page 2, line 37). This is true only if such actions are specified in the vendor's SLA.

(Page 3, lines 9-10). This was discussed on an earlier SCRM SDT call, if a vendor can demonstrate that it is certified by ISO or some other certification organization, it may provide a statement to that effect, in lieu of specific agreements with each customer. This issue may still be fluid, but should be included in the final Guidance, as well, in order to satisfy FERC's directive to not extend CIP-013-1 beyond the purview of Section 215 to vendors.

(Page 3, lines 29-30). It appears the key element in this passage is to ensure entities have implemented a sound SCRM program and suitable processes to mitigate vendor risk, it does not require entities to take extraordinary measures to ensure all such processes are included in final SLAs.

(Page 3, lines 42-44) We can reasonably expect most, if not all, SCRM plans to follow the guidelines below to incorporate applicable controls into the plan. However, these suggested controls are best practices, but not mandatory controls. Entities can use these guidelines as an initial starting point for the development of the SCRM plan, as can the Regional Entities for review and evaluation of the R1 SCRM plan at audit..

(Page 4, footnote 1). This footnote cites a third party commercial product. WECC's approach to maintaining auditor independence includes its position to never endorse, recommend, or otherwise indicate favorite vendor status to any consultant, vendor, or product. As a result of this approach, WECC does not consider it appropriate to recommend or endorse a specific tool such as this product.

(Page 5, lines 34-37). This bullet addresses the potential for contractual controls for SCRM that stems from a sound RFP process and procedures. If an entity takes this approach, WECC would expect to see an RFP template that includes specific cyber security terms and expectations. We would then sample for completed RFPs to evaluate the entity's implementation of this approach.

(Page 6, Section 1.2.1 line 4). Unless these processes are specifically included in a vendor SLA or other binding document, it will be difficult for a Regional Entity to evaluate anything other than the entity's plan for such notifications. Since the burden of proof cannot be passed along to the vendor other than through contract, the audit of most of these 1.2.x sections may generally be nothing more than a review of the entity's plan.

(Page 10, lines 6-7). Communications and training materials relative to SCRM should also be addressed in the entity's overall Cyber Security Awareness program.

(Page 13, R4). As mentioned in the R4 comments above, this is a major security concern from WECC's perspective and should leverage and expand upon an entity's controls and procedures for Interactive Remote Access [IRA] from CIP-005-5 R2.

(Page 16, R5). An entity can leverage its R3 and R4 controls to support R5, but it is not required to do so. However. based on prior discussions with entities relative to CIP-010-2 R4, in practice, WECC would expect to see implementation efforts of this nature relative to SCRM controls for Low-impact BCS.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Currently, implementation guidance is imbedded in the Technical Guidance document covering what the Standard means, and how to implement it. Southern requests that those topics be separated out.	
Likes 0	
Dislikes 0	
Response	

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

PSEG appreciates the standard drafting team's effort in providing technical guidance and examples to provide additional clarity and implementation support for the registered entities. PSEG has the following questions/recommendations to the Technical Guidance and Examples document below:

- The term vendors as used in the standards is defined (Page iv Line 6) in the Technical Guidance and Examples document (as well as in the Rationale for Requirement R1 in the draft CIP-013 Standard). This term should be officially defined in the Glossary of Terms used in NERC Reliability Standards.

- Page 4, line 37: Add the wording "as determined by the Registered Entity" after the word components. The new statement would state, "Define any critical elements or components, as determined by the Registered Entity, that may impact the operations or reliability of BES Cyber Systems". This change aligns with the FERC order (p31) statement that the standard should have flexibility to account for varying " differences in the needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risks" to determine the critical elements and components that may impact operations or reliability of BES Cyber systems based on the registered entities implementation of a vendor system or component within their program.

- Page 5, line 24: Add the wording "as identified by the Registered Entity" after the word "risks". The new statement would state, "Review and address other risks as identified by the Registered Entity in Requirement R1 Part 1.1.1." Recommend this change to align with the change to technical guidance for Requirement 1.1.1 (Page 4, line 37) above.

- Page 6, line 43: Replace the word "breaches" with "vulnerabilities and threats" to align with the use of the word "vulnerabities" in the requirement language.

- Page 7, line 1: Replace the word "breach" with "vulnerability" to align with the use of the word "vulnerabities" in the requirement language.

- Page 7, line 9: Remove the words "availability or". The NERC CIP reliability standards require protecting BES Cyber Systems to support reliable operation of the BES. Recommend removing availability to align with the wording used throughout the NERC CIP reliability standards.

- Page 13, line 9: Recommend changing Requirement 4.3, from "Disabling or otherwise responding to unauthorized activity during remote access sessions"to "Disabling or otherwise responding to detected unauthorized activity associated with remote access sessions." (see comment under question 4)

- Page 15, line 22: Recommend adding the word “detected” to align with the recommended changes to Requirement 4.3. The statement would become “Set up alerting and response processes so that detected inappropriate vendor remote access sessions may be disabled or otherwise responded to in a timely manner.

- Page 15, line 23: The words “in a timely manner” are overly subjective. Recommend specifying a specific time frame for a timely response.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Response

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

AZPS requests clarification that the Technical Guidance and Examples being incorporated into the Standard will be used as technical guidance only, and not compliance guidance.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mike Smith - Manitoba Hydro - 1

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
There is inconsistency with the language of the Requirements and the Technical Guidance language, specifically in reference to Requirement R3 and Requirement R4. The guidance sections for both Requirements mention reviewing security policies, however, the Requirements mention Risk Management Plans. NRG suggests that this language be properly aligned or else this could lead to future Compliance Enforcement issues for the industry. NRG requests SDT clarity that system-to-system is equivalent to machine-machine.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	

On Page 9, line 43, the Technical Guidance and Examples references the use of industry best practices and guidance that improve cyber security risk management controls. This does not match the rationale of R2 which only speaks to the use of guidance. Exelon feels that the reference to “industry best practices” should be removed from the Technical Guidance and Examples since it is non-specific and open to interpretation.

Likes 0	
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	
Document Name	

Comment

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or, define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be either defined in this standard or in the NERC Glossary of Terms. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition. The “threatened, attempted” part of this definition would is too large in scope and could require large vendors like Microsoft or Cisco to report thousands or millions of attempts each day. Suggest replacing “vendor security event” in R1.2.1 with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Page 6, line 12: It is unclear that the R1.2.1 requires notification by the entity to the vendor.

Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Page 16 line 25, replace “should” with “may”.

Suggest adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging

In other standards, the Guidelines and Technical Basis document is included in the standard, suggest that this also be completed for CIP-013.

Likes 0	
Dislikes 0	

Response

Romel Aquino - Edison International - Southern California Edison Company - 3

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE has no comments for this question.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	

Document Name	
Comment	
We did review the TG&E document briefly and it was valuable in illustrating how some of the team members were viewing various requirements; however, it will need to be further refined once the changes are made to the requirements. We did note that in the discussion of integrity and authenticity, there was a lot of duplication in methods between the two making it seem that there might be some fuzziness on what each of the two descriptors are trying to address.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	
Document Name	
Comment	
- See APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Response	
Glenn Pressler - CPS Energy - 1	
Answer	

Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Response	

9. Provide any additional comments for the SDT to consider, if desired.

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	

In voting “no” on this proposed Reliability Standard, MRO acknowledges the impossible challenge faced by the Standard Drafting Team and NERC in developing a Supply Chain Reliability Standard as directed in FERC Order No. 829 issued July 21, 2016. Federal Energy Regulatory Commission (FERC) Acting Chairman LaFleur (then a commissioner), stated in her dissenting opinion, “[E]ffectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, economic, and business relationship issues.”

As a regulator, MRO seeks to provide clarity about Reliability Standard requirements, assurance around compliance with those Reliability Standards, and results – reduced risk to the reliable operation of the bulk power system (BPS). Adoption of the proposed Reliability Standard will not meet these goals.

The proposed Reliability Standard directs registered entities to complete tasks that require agreement of vendors that are not subject to the jurisdiction of the FERC or the Electric Reliability Organization (ERO). To accommodate this lack of jurisdiction, the proposed Reliability Standard is drafted sufficiently vague to allow for lack of vendor agreement and compliance with the Reliability Standard to exist at the same time. For example, Requirement 1 of CIP-013 obligates registered entities to implement supply chain risk management plans. At the same time, the supporting Rationale states, “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement the entity’s plan.” In essence, this Requirement forces entities to develop a plan, but a failure to be able to implement the plan is not an issue of noncompliance. The root cause of the problem is that the risk lies with vendors, a third party not subject to FERC or ERO jurisdiction. Thus, the Reliability Standard becomes more paperwork and administrivia than mitigation of risk. See the comments of the MRO stakeholder-driven NERC Standards Review Forum.

As a regulator, MRO believes the proposed Reliability Standard cannot be effectively and efficiently assessed and therefore MRO would not be able to provide assurance of compliance or, more important, assurance of reduced risk to the reliable operation of the BPS. As drafted, MRO will be expected to determine if registered entities made a reasonable attempt to address supply chain risks through their procurement processes. Since contracts are always a give and take with regard to a number of provisions, how does a regulator efficiently and effectively monitor one aspect of the contract negotiation process to determine reasonableness and the possible existence of countermeasures to address security throughout the procurement process which may be beyond our jurisdiction and rest with best security practices?

In addition, the draft Reliability Standard does not address supply chain management comprehensively. For example, the issues associated with vendors of the vendors are not addressed. It is very common for an Energy Management System (EMS) vendor to deliver a system with third party software, such as Adobe®, Java, or even open-sourced software such as PuTTY. The vendor chain for any system can be deep and the proposed Reliability Standard does not provide registered entities clarity on how to deal with these routine layers of vendors.

Finally, it is also important to consider the potential economic impact on future contract negotiations between registered entities and vendors. The proposed CIP-013 directs a registered entity to address supply chain risks in its vendor contracts. How much does the registered entity pay to manage supply chain risk when the vendor has no legal obligation to accommodate the registered entity? By placing additional requirements on vendors, do we unintentionally reduce competition, increase costs, and reduce innovation? Furhtermore, the possibility of less competition, creates less diversity across the bulk power system and less diversity increases risk.

Reducing supply chain risk to the reliable operations of the BPS and providing the requisite regulatory assurance that that risk has been reduced is a complex task for the very reasons FERC Acting Chairman LaFleur communicated in her dissent. Whether or not this risk is best addressed by a NERC Reliability Standard as opposed to a security framework, an IEEE standard or use of military grade components merits greater consideration. This is particularly true given four of the five FERC commissioners will have either not considered or not supported FERC Order 829 when the proposed Reliability Standard is ultimately filed with FERC. Following the comment period, MRO recommends that FERC and the ERO consider whether we have

the appropriate structure and expertise to address and mitigate this risk that resides with vendors effectively and efficiently through a Reliability Standard.	
Likes 2	Platte River Power Authority, 5, Archie Tyson; Gresham Darnez On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1,
Dislikes 0	
Response	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The NSRF has concerns with being held accountable for a vendor who does not meet the attributes of this proposed Standard, especially for entities that have Low Impact BES Cyber Systems, only. Many of the entities that have Low Impact BES Cyber Systems only, are small (read low risk) entities that may have one Low Impact BES Cyber Systems (maybe a generator, one Transmission substation, or control system). How is the small entity going to stand up to large multi-regional corporate companies (i.e. the vendor), when the vendor will not comply with the requirements of the small entity (and CIP-013-1)? The Low Impact BES Cyber Systems entity will carry all the compliance risks (burden) when they find out that the vendor did not comply with said requirements, regardless of how the entity will ensure that the vendor will comply, a contract, statement of work, etc. If the vendor does agree with supplying proof that is requested, the small entity will then incur **more cost** (read increase costs) to the Low Impact BES Cyber Systems entity by being found non-compliant. The entity may not be able to recoup that cost due to the rate structure of that entity's state commission. This may lead the small entity to assume more risks because the cost is too great and not have a system fully protected. They would be fully compliant by writing their plan and stating everything is low risk and controls are not required. The guidance document suggests not making these requirements contractual language as it makes negotiations more difficult. This puts us in a poor situation as we are required to do it but don't get NERC support via a requirement in the standard to force the agreement to stipulate it. If it was part of the standard to require it, it would give all Responsible Entities consistent leverage to utilize as all would require it. NERC should provide the areas that should be covered in an agreement in a standard format to provide consistency. The Standard does not make it clear how any cloud based services may be impacted by this standard. We suggest the SDT to consider how this standard may apply to cloud based systems and provide any relevant clarifications.	
Likes 2	Platte River Power Authority, 5, Archie Tyson; OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Response	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	

No additional comments.

Likes 0	
Dislikes 0	

Response

Donald Lock - Talen Generation, LLC - 5

Answer	
Document Name	

Comment

We are concerned that CIP-013-1 may oblige entities to purchase equipment that doesn't presently exist and may never exist, and to take actions that are impossible. The standard should at a minimum state that it does not require NERC entities to:

- impose cyber security measures or reporting on the suppliers of programmable electronic devices (PEDs),

- monitor vendors to ensure that they are properly implementing their cyber security programs,

- ensure that as-received software and firmware is in the as-shipped condition.

- eliminate risk (only mitigation of risk is possible).

It would be impractical for vendors to individually negotiate a unique CIP agreement with each purchaser, and the net effect on BES reliability could be negative if the current vendor (for NERC entities with standardization programs) or the vendor with the best product (for competitive bidding) chooses not to develop CIP-013-friendly products due to the burden of compliance. We would support a qualification program administered by a NERC-approved central authority, however, such that entities could address supplier-related issues simply by purchasing CIP-013-certified products.

A blanket allowance is needed for entities to take technical feasibility exceptions (TFEs), to address the wide variety of PED types and to address instances of vendors not producing the inputs that entities are supposed to act upon.

CIP-013-1 as presently written may create extreme reluctance to enhance plants in accordance with technological developments, which again would be counterproductive regarding long-term BES reliability.

Likes 0	
Dislikes 0	

Response

Marty Hostler - Northern California Power Agency - 5

Answer	
Document Name	

Comment

See APPA's, TAP's, and USI's comments.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5

Answer	
Document Name	

Comment

AEP believes the SDT should specifically mention CIP Exceptional Circumstances in the Standard in order to clearly identify that entities would be exempt from complying with CIP-013-1 in the event of a qualifying CIP Exceptional Circumstance.

In addition, Order 829 specifically mentions that the Standard should be forward-looking, but CIP-013-1 does not mention it. AEP believes the SDT should revise CIP-013-1 to include a statement in alignment with FERC's directive that this Standard should be forward-looking.

Likes 0	
Dislikes 0	

Response

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3

Answer	
Document Name	

Comment

Please modify this standard using the similar 'Applicability' table format used in the earlier standards.

This set of base requirements is would duplicate effort on the part of each entity to evaluate Supply Chain risk for vendors that provide the same product to multiple entities. Some consideration should be given to creating a standard review, application or qualification form that vendors can complete to certify their product and its delivery.

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	

There is significant overlap to CIP-005, 007, 008, 010. If the intent is to impose additional requirements on the procurement process those requirements should be integrated into the appropriate standard to maintain the linkage. Duplication of requirements in another standard will only create confusion and wasted effort for entities to meet CIP compliance.

The requirements as written are not consistent with the standard's stated purpose: "To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems." This purpose statement indicates this standard is intended to address items that should be considered during the procurement/contract negotiations process and included in terms of the contracts. The requirements as written imply that enforcement of the terms of the contract will be audited. The lifecycle management is currently addressed in CIP-005, 007, 008, 010.

The applicability of each of the requirements is not clearly addressed. Standards CIP-002 through CIP-011 clearly define the applicability for each requirement and sub-requirement.

2. Suggest include supply chain certifications such as ISO-28000 and Customs-Trade Partnership Against Terrorism certification as items to ask for in request for purchase.

Likes 0	
Dislikes 0	
Response	

Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	
Response	

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	
Document Name	

Comment
R1.2.6 states the RE needs to provide "*Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s);"* While R4 and R5 require *"Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)."* Different terms regarding obligations for vendor remote access have been used with regard to R1.2.6 than under R4 and R5 (e.g., "coordination" and "controlling:"). We seek clarification on whether that is intentional. If the two terms are intentionally different, more clarity is needed on what different obligations are being imposed between R1.2.6 and R4/R5. If R1.2.6 and R4/5 are not meant to impose different obligations, we suggest use of consistent terms or wording.

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Response

Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	

Comment
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison

Likes 0	
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	
Document Name	

Comment

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	
Document Name	

Comment

PRPA understands that the SDT is under time constraints in addressing Order No. 829, however, PRPA requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

PRPA requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

PRPA feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to PRPA if this was intentional for R3 and R4. PRPA requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Response

Steven Mavis - Edison International - Southern California Edison Company - 1

Answer	
Document Name	

Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	
Document Name	

Comment

AE understands that the SDT is under time constraints in addressing Order No. 829, however, AE requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

AE requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

AE feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to AE if this was intentional for R3 and R4. AE requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	

Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments including modifications to existing contracts and agreements to deliver desired solutions. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

Moify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

Move CIP-013 R2 into CIP-003-x R1 with other CIP policies that are reviewed by the CIP Senior Manager. This would also provide alignment across high, medium, and low impact Cyber Assets.

CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	
Document Name	
Comment	

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	
Document Name	

Comment

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3

Answer	
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Response	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC

Answer	
Document Name	
Comment	
As written, implementation of this draft standard may degrade rather than improve reliability by interfering with the ability to respond and recover from BES cybersecurity events. The draft standard also encourages the use of a monoculture of products allowing broader damage from a single zero-day vulnerability.	
Likes 0	
Dislikes 0	
Response	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Response	

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable

Answer	

Document Name	

Comment

The American Council of Engineering Companies (ACEC) -the business association of the nation's engineering industry - wants to convey the industry's perspectives and concerns over the development of this new cyber security supply chain rule mandated by the Federal Energy Regulatory Commission (FERC).

ACEC member firms, numbering more than 5,000 firms representing over 500,000 employees throughout the country, are engaged in a wide range of engineering works that propel the nation's economy, and enhance and safeguard America's quality of life. Council members are actively involved in every aspect of the energy marketplace.

Supply chain cyber security is of growing concern to all our members. While we believe that present cyber security controls and voluntary practices are highly effective, input by engineering service providers would assist NERC/FERC in producing a more effective approach in minimizing the impacts on competition, risk allocation, and pricing.

In short, ACEC is in agreement with most of the comments of the owners, operators, vendors and suppliers that have formally participated in this Standard development. We fully appreciate the concerns over how risk can be adequately managed under any proposed standard. Our member firms' reputations depend upon professional performance and innovation in an atmosphere of collaboration. However, we are concerned that the supply chain language in this Standard will not support, and may actually impair, broad-based cost-effective infrastructure security and grid reliability

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	
Document Name	

Comment

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor’s inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states “suppliers, vendors and other entities”. The Requirement language only references vendors. The SDT should clarify who or what “suppliers” and “other entities” are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

SRP understands that the SDT is under time constraints in addressing Order No. 829, however, SRP requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

SRP requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor’s inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

SRP feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states “suppliers, vendors and other entities”. The Requirement language only references vendors. The SDT should clarify who or what “suppliers” and “other entities” are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to SRP if this was intentional for R3 and R4. SRP requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Response

Kenya Streeter - Edison International - Southern California Edison Company - 6

Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	
Document Name	
Comment	
FirstEnergy recommends that the SDT take additional time in preparing a draft supply chain Standard that properly separates “supply chain” Requirements from additional operational and maintenance Requirements. Operational and maintenance Requirements should be added to the existing CIP Standards where the subject protections are already addressed. In addition, any Requirements applicable to Low Impact BES Cyber Systems should be placed in CIP-003 as has been established as a practice for all other low impact requirements. It should also be noted that certain expectations of these Requirements have economic implications to entities of all sizes. These Requirements could result in limiting the flexibility of an entity to obtain cyber assets from third-party distributors at a significant discount. For some entities, the additional costs could have an impact on their ability to remain for example, an economically viable generating unit. While probably not something that by itself impact the continued operation of a generating unit, the additional costs associated could be an influencing factor in keeping BES generating unit in-service.	
Likes 0	
Dislikes 0	

Response
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1
Answer	
Document Name	
Comment
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).
Likes 0	
Dislikes 0	
Response
Mike Kraft - Basin Electric Power Cooperative - 5
Answer	
Document Name	
Comment
Basin Electric has concerns with being held accountable for vendors who not meet the attributes of this proposed Standard. Basin Electric prefers existing CIP standards be modified to satisfy the order. With the current FERC Commission lacking quorum, the timeframe to add commission members and the resulting backlog from the delay, it would appear the FERC Commission is not in a position to act upon a hastily constructed new standard. Basin Electric suggests NERC request an extension of time to modify existing standards to meet the order. Basin Electric suggests CIP-013 follow the table structure used in the existing enforceable CIP standards including the Part, Applicable Systems, Requirements and Measures.
Likes 0	
Dislikes 0	
Response
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison
Answer	
Document Name	
Comment

Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

Move CIP-013 R3, to CIP-010 R1.

CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

Move CIP-013 R5 to CIP-003 R2

Question – what about contracts negotiated during the implementation period? Are these contracts subject to this Standard? What about existing contracts? What about contracts that are renewed (evergreen contracts)? What about contracts initiated during the 15 calendar month review?

Likes 0	
Dislikes 0	

Response

Michael Ward - Seminole Electric Cooperative, Inc. - 4

Answer	
Document Name	

Comment

Seminole Electric comments submitted by Michael Haff

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx

Comment
See comments in the attached file.

Likes 0	
Dislikes 0	

Response

Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	
Document Name	

Comment
PJM agrees with the comments submitted by the SWG. Additionally, PJM suggests that 1.2.1 be stricken since it is ambiguous and already covered by 1.2.3 and 1.2.4. It is not clear what would be defined as a “vendor security event” that is outside of the events listed in 1.2.3 and 1.2.4.

Likes 0	
Dislikes 0	

Response

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	
Document Name	

Comment
“This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.” - Verbiage to this effect needs to be part of the standard. Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event. Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Fred Frederick - Southern Indiana Gas and Electric Co. - 3

Answer	
Document Name	

Comment

Verbiage similar to the follwoing needs to be part of the standard. “This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.”

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	
Document Name	

Comment

Summary of comments direction:

1. No “plans.” (Delete R1 and R2). Order 829’s four objectives did not include creating “plans.”

2. All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011. (Delete R3-5).

3. We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

Result: No CIP-013 standard. Revised CIP-002 through -011 standards.

Other comments:

On the one hand Order 829 states intent to respect FPA section 215 jurisdiction by only addressing the obligations of responsible entities. A Reliability Standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities.

Yet, in paragraph 59, Order 829 states, "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."

Contracts are bi-lateral and as such impose obligations on both parties, in direct contradiction to not imposing obligations on suppliers, vendors or other entities. Paragraph 59 is indirectly imposing obligations on suppliers, vendors or other entities that provide products or services to responsible entities.

If the entity chooses, contracts can be a tool in "how" they deliver the "what" for the security objective. However, the registered entity's compliance has to be measured on achieving the security objective, not on contract terms.

We will not support any standard that prescribes contract terms and makes contract terms a measure of an entity's compliance. Entities have been achieving the CIP-004 security objectives for background checks, training and access revocations since CIP version 1 without the prescription of "how" it had to be done (without making contract terms a measure of their compliance).

We strongly agree with the Midwest Reliability Organization comments.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Response

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	
Document Name	
Comment	

"This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement." - Verbiage to this effect needs to be part of the standard.

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	
Response	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	
Document Name	
Comment	

- During the Assess/Plan, Procure/Acquire phases of the Supply Chain process, separate requirements for standalone Standard (CIP-013) should be developed. For the deployment and operational aspects of the Supply Chain, appropriate requirements should be incorporated into the existing CIP Standards. It is recommended that this SDT collaborate with the CIP-002-CIP-011 SDT for language that can be used until R3 – R5 can be moved to their appropriate operational standards.
- All measures sections will need to be updated to reflect any changes that are made to the requirements.
- Dominion recommends that "remote access" should be changed to "electronic remote access" throughout the proposed CIP-013-1.

Likes 0	
Dislikes 0	

Response

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	
Document Name	

Comment

The need to have supply chain risk management is agreeable; however, in its current form, CIP-013-1 poses a great challenge and burden to SCE&G and other Responsible Entities for various reasons, many of them documented in the Unofficial Comment Form. SCE&G recommends that CIP-013-1 include a modified R1 and R2 only, and not include R3 through R5. Requirements R1 and R2 focus on the supply chain and will suffice as an initial implementation step of supply chain risk management. The remaining requirements are operational obligations that need to be integrated into existing NERC CIP Standards.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	
Document Name	

Comment

Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standards.

Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Also recommend the following:

- Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.
- Move CIP-013 R3, to CIP-010 R1.
- CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6
- Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5

Answer	
Document Name	

Comment

No comments.

Likes 0	
Dislikes 0	

Response

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	
Document Name	

Comment

Request verbiage similar to the following is added as part of the standard:

This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	
Document Name	

Comment

{C}1) Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

{C}2) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

{C}3) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

{C}4) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

{C}a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

{C}b. Move CIP-013 R3, to CIP-010 R1.

{C}c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

{C}d. Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	

Comment

In the Purpose, change “security controls” to “procurement and operational controls” as presented in the materials.

CenterPoint Energy request that the SDT format CIP-013 like the other CIP Standards, a table design, if possible.

CenterPoint Energy suggests more collaboration between the CIP Modifications SDT and the Supply Chain SDT to help eliminate overlap and better align with existing CIP requirements.

In general, the SDT should consider the operational impacts that this standard could have on the industry. Flexibility is necessary.

Likes 0	
Dislikes 0	

Response

Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	

HQT voted Negative and would like to see the following matters to be addressed:

-CIP-013 should move forward with only R1 and R2 since they are mostly procurement related-some concern is being expressed that the requirements for having a supply chain risk management plan seem to a cover low medium and high BES Cyber assets as well as allowing entities to assess their own risk. Further clarification and perhaps some third party verification would be beneficial.

-Contractual issues could exist. Although the FERC order doesn't require abrogation of contracts there is some concern that there could end up being multiple contracts in place, those newly negotiated and the existing ones. Confusion exists between use of terms vendor and suppliers in the draft standard and the Guidance section.

-Concerns exist regarding authentication on multiple levels and how vendors and their manufacturers may combine hardware and software into their products and how there could meaningful verification and authentication

-There are a number of areas where time seems to be an issue as it relates to implementation

-Use of "applicability tables" as they appear in other CIP standards would clarify the requirements to alleviate compliance concerns

- R3, R4 and R5 should move into existing CIP Standards to avoid P81 issues (redundancies) and ease implementation for Entities and improve auditability efficiencies.

Likes 0	
Dislikes 0	
Response	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	
Document Name	
Comment	

OUC understands that the SDT is under time constraints in addressing Order No. 829, however, OUC requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

OUC requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Likes 0	
Dislikes 0	

Response

Lauren Price - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

In conclusion, ATC has concern that, despite what is a well-intended attempt by a highly qualified SDT to address the directives of FERC Order 829, CIP-013-1 is its current form is ultimately serving as an vehicle to revise or expand the scope and requirements to several currently approved and enforceable CIP Cyber Security Reliability Standards without affording the industry due process in accordance with the NERC Rules of Procedure for those modifications. 1.) Where existing Reliability Standards and Requirements meet the intent of CIP-013-1 and the FERC Order 829 directives, the existing Reliability Standards should be leveraged to accomplish the objective instead of creating a duplicative standard. 2.) Where Reliability Standards and Requirements may not go far enough to meet a given objective as it relates to vendors or suppliers, consideration should be given to modifying those existing Reliability Standards and Requirements, or perhaps investing time toward the further exploration of leveraging available standardized industry frameworks or practices that meet the objectives in an ever changing threat landscape as opposed to a reliability standard that a.) may be ill-equipped to keep pace with emerging threats and b.) perhaps carry the risk of hindering a Registered Entity's ability to be timely and nimble in addressing those threats in order to maintain compliance with a requirement(s) that has been rendered irrelevant. The creation of a new Reliability Standard should not supersede, contradict, expand, amend, or otherwise effectively revise other currently approved and enforceable CIP Cyber Security Reliability Standards. Those Standards exposed to this condition are cited in other comments and include, at a minimum the below listed five (5) CIP Standards:

- CIP-002-5.1
- CIP-003-6
- CIP-004-6
- CIP-005-5
- CIP-007-6

In conclusion, the above concerns related to redundancy or contradiction to approved and enforceable CIP Standards, the cited expansion to the FERC directives, and the confusion, inconsistency, and broad sweeping language that is at odds with the intent of both enforceable CIP Standards, the effort of paragraph 81, and FERC Order 829 supports the wisdom and caution within FERC Commissioner's (Cheryl A. LaFleur's) dissent to FERC Order 829. LaFleur's dissent to FERC Order 829. (P. 67) issued on July 21, 2016, cautions that "**…effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, technical, economic, and business relationship issues**." In this dissent, LaFleur acknowledges that the threat of inadequate supply chain risk management procedures poses a very real threat to grid reliability; and while LaFleur offers full support of the Commission's continued attention to this threat, LaFleur's **"…fear that the flexibility** *[within FERC Order 829]* **is in fact a lack of guidance and will therefore be a double-edged sword.**" is demonstrable in this first draft of CIP-013, and further evidence that FERC Order 829 may have been premature thereby causing a highly qualified and well-intended SDT to be ill-equipped to "**…translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act.**" With

Cheryl A. LaFleur's recent appointment to FERC's Acting Chairman on January 23, 2017, ATC respectfully encourages NERC and the SDT to consider if there is an opportunity for FERC to revisit the need for the CIP-013-1 Supply Chain Reliability Standard and to reevaluate the appropriateness and viability of FERC Order 829 and whether or not the SDT should move forward or if FERC Order 829 should be rescinded in favor of the industry leveraging the existing CIP-002 – CIP-011 approved and enforceable reliability standards in combination with the risk-based industry standards and frameworks as an alternative approach to drafting this new Reliability Standard. ATC thanks the SDT for consideration of our positions.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE

Answer	
Document Name	

Comment

1. We believe in finding a beneficial multi-sector solution that will lower costs, encourage innovation, and support among multisector vendors.

2. The current standard would create a compliance burden for entities that are already resource constrained.

3. We believe that the SDT should focus on a supply chain management standard that is designed to:

· Manage in addition to eliminating risk;

· Ensure that operations are adapting to constantly evolving threats;

· Be aware of and responsive to changes within their own organization, programs, and the supporting information systems; and

· Adjust to the rapidly evolving practices of the electricity sector's supply chain.

4. Though the current language would certainly raise standards across the entirety of the software industry, it could result in isolation of the electricity sector and hamper growth and innovation among industrial control vendors.

5. We thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	

Reclamation commends the SDT for the draft that was provided for a new and complex standard in a short amount of time.

Reclamation recommends a more simplified format of the proposed standard.

Reclamation believes that the objectives and intent and of FERC Order 829 can be met without spelling out each objective as a separate requirement. As presently written, the first draft contains repeating elements (such as access, authentication, product delivery, etc.) in different requirements. The simplified approach described in the answers to Questions 1 through 5 above would eliminate redundancy.

Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	

Santee Cooper understands that the SDT is under time constraints in addressing Order No. 829, however, the SDT should carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Santee Cooper requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Santee Cooper recommends that all standards with requirements that apply to low impact assets be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear if this was intentional for R3 and R4. Santee Cooper requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Santee Cooper recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, Santee Cooper agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and Santee Cooper urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address gaps remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns that does not advance the security of the grid, as set out by now-Chairperson LaFleur in her dissent to Order 829.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
FERC Order no 829 (p21) discusses “suppliers, vendors and other entities”. CIP-013-1 only refers to vendors. BPA suggests that the SDT clarify the scope and define any appropriate differences applicable to supplier, vendors or other entities.	
Likes 0	
Dislikes 0	
Response	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	

Document Name	

Comment

1) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

2) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

3) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments including modifications to existing contracts and agreements to deliver desired solutions. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

b. Move CIP-013 R2 into CIP-003-x R1 with other CIP policies that are reviewed by the CIP Senior Manager. This would also provide alignment across high, medium, and low impact Cyber Assets.

c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

d. Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Response

Glenn Pressler - CPS Energy - 1

Answer	
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Response

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	
Document Name	
Comment	

Colorado Springs Utilities (CSU) understands that the SDT is under time constraints in addressing Order No. 829, however, CSU requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CSU requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CSU feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CSU if this was intentional for R3 and R4. CSU requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

CSU requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although

the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
While there are different ways to approach the complex issues of the supply chain risk, a proactive approach to address the issue can only help improve the industry's security posture. The difficulty in addressing the complexities requires additional evaluation to address the issues impacting both the development and implementation of solutions. Similar to CIP-014, the development of Supply Chain Risk Management plans and procurement process proposed under R1 and R2 may be appropriate within a new or revised Reliability Standard. The technical controls proposed for CIP-013 R3 and R4 may be better addressed within existing CIP Standards. The IESO abstains from commenting on R5 but believes integration into existing CIP Standards might be appropriate, especially since CIP-003 Attachment 1 already is comprised of a security plan. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. This is applicable to Requirements 1, 3, 4, and 5. The plan should allow for risk acceptance and leverage of an exception process. To address these concern, the drafting team should include some provisional or exception language to protect Responsible Entities such as use of a Technical Feasibility Exception (TFE). NERC's Appendix 4D to the Rules of Procedure provide for a basis of approval of a TFE beyond strict technical limitations of a system. Reference Section 3.0 of the appendix for more information. The Standard uses "supplier" and "vendor" throughout, interchangeably. The terms should be consistent throughout to avoid confusion.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx
Comment	
The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.	

Seattle City Light understands that the SDT is under time constraints in addressing Order No. 829, however, Seattle City Light requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Seattle City Light requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively, this could be addressed as an Exemption in Section 4.2.3.

Seattle City Light feels that all standards with requirements that apply to low impact assets should be included in CIP -003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to Seattle City Light if this was intentional for R3 and R4. Seattle City Light requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

As discussed in comments to R1 above, Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.

Seattle City Light recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, City Light agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and City Light urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address the gaps that remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns. Thus this standard "does not advance the security of the grid," as set out by now-Chairperson LaFleur in her dissent to Order 829.

Likes 0	
Dislikes 0	

Response

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	
Document Name	

Comment
FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	

Response

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	Hydro One_Unofficial_Comment_Form_CIP-013-1-First Draft.docx

Comment
We suggest that the standard should have two requirements only. R1 could require the entities to identify risks, evaluate controls (at minimum the controls itemized in FERC Order), and implement controls based on the acceptable level of risk to address the four objectives in FERC Order and mitigate risks stated in the Order. R2 could be the periodic review and approval of R1 by CIP Senior Manager. The applicability could be to all BES Cyber Systems essential for operation of BES. Entities should consider impact rating of High, Medium and Lows when evaluating necessary controls. **Comment for consideration in the RSAW** For the RSAW and under Requirement 1 in the section called “Note to the Auditor”, We recommend adding that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” as stipulated in the Rationale for Requirement 1.

Likes 0	
Dislikes 0	

Response

Erick Barrios - New York Power Authority - 5	
Answer	
Document Name	

Comment
The NYPA Comments

Likes 0	
Dislikes 0	

Response
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	
Document Name	

Comment
SMUD understands that the SDT is under time constraints in addressing Order No. 829, however, SMUD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1. SMUD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3. SMUD feels that all standards with requirements that apply to low impact assets should be included in CIP -003. As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard. Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to SMUD if this was intentional for R3 and R4. SMUD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI members prefer use of the applicability tables, especially for R3 and R4.

EEI commends the work done by the SDT and NERC on this difficult task. CIP-013 is a challenging standard given it is focused on minimizing risk introduced by third parties that the Responsible Entities have little control over. In particular, we are reminded of Acting Chairman LaFleur's dissenting statement "effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, economic, and business relationship issues."

In addressing our comments and others, we recommend that the SDT focus on the security objectives and what the Responsible Entities can do in procurement to minimize risk to the bulk-power system. Although cybersecurity is a risk, other risks such as reliability may outweigh the need for certain cybersecurity focused requirements. Cybersecurity is about managing risk, which must be balanced against a number of factors and for the electricity subsector, keeping the lights on is key.

Likes 0	
Dislikes 0	

Response

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3

Answer	
Document Name	

Comment

Tacoma concurs with the comments provided by the LPPC.

Likes 0	

Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	
Document Name	

Comment

BANC supports the comments filed by Sacramento Municipal Utility District

Likes 0	
Dislikes 0	

Response

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	
Document Name	

Comment

While there are different ways to approach the complex issues of the supply chain risk, a proactive approach to address the issue can only help improve the industry's security posture. The difficulty in addressing the complexities requires additional evaluation to address the issues impacting both the development and implementation of solutions. Similar to CIP-014, the development of Supply Chain Risk Management plans and procurement process proposed under R1 and R2 may appropriate within a new or revised Reliability Standard. The technical controls proposed for CIP-013 R3 and R4 may be better addressed within existing CIP Standards. The IRC abstains from commenting on R5 but believes integration into existing CIP Standards might be appropriate, especially since CIP-003 Attachment 1 already is comprised of a security plan.

This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. This is applicable to Requirements 1, 3, 4, and 5. The plan should allow for risk acceptance and leverage of an exception process. To address these concern, the drafting team should include some provisional or exception language to protect Responsible Entities such as use of a Technical Feasibility Exception (TFE). NERC's Appendix 4D to the Rules of Procedure provide for a basis of approval of a TFE beyond strict technical limitations of a system. Reference Section 3.0 of the appendix for more information.

The Standard uses "supplier" and "vendor" throughout, interchangeably. The terms should be consistent throughout to avoid confusion

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	

We appreciate the significant efforts of the SDT to develop this draft standard on difficult subject matter in such a short amount of time. However, based upon this initial draft, it is evident that additional time is necessary for the SDT to develop an effective standard addressing supply chain security risks. We suggest that the SDT develop a formal recommendation to NERC staff requesting that NERC file for an extension of time to collect additional stakeholder feedback in order to develop a more effective standard.

In general, we request that the SDT consider our comments in question 1 that supply the following framework for a supply chain security standard:

FERC's directives in paragraphs 43 through paragraph 62 summarized a general framework for this new Standard as outlined:

R1: Develop a plan to include security controls for supply chain management that include the following four specific security objectives in the context of addressing supply chain management risks:

R1.1 Security objective 3 (*information system planning*)

R1.2 Security objective 4 (*vendor risk management and procurement controls*)

R1.3 Security objective 1 (*software integrity and authenticity*)

R1.4 Security objective 2 (*vendor remote access*)

R2: Implement the plan specified in R1 in a forward looking manner.

R3: Review and update, as necessary its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months

R3.1 Evaluation of revisions…

R3.2 Obtaining CIP Senior Manager or delegate approval.

GTC feels this framework outlined above satisfies Order 829 in the context of addressing supply chain management risks, completely. Although FERC expressed some operational scenarios of existing CIP standards not explicitly addressing supply chain risks, the point of FERC's summary was still in the context of addressing supply chain risks and not additional operational controls as presented by the SDT.

From a clarity standpoint, we urge the drafting team to consider limiting the structure of CIP-013-1 to the supply chain horizon which ends at the delivery of products/services to the acquirer in accordance with NIST SP 800-53 r4 rather than a holistic BES Cyber System Life Cycle approach chosen. GTC submits that the operations and maintenance of BES Cyber systems are already addressed in existing standards. Lastly, FERC provides NERC

discretion per paragraph 44 the option of modifying existing Reliability Standards to satisfy the directive, so if the SDT believes additional operational gaps still exist, then GTC prefers NERC identify these risks, and explain to FERC NERC's intent to invoke operational changes by modifying existing CIP requirements with the submission of a "supply chain horizon contained" CIP-013-1.

Lastly, GTC recommends the SDT develop a Guidelines and Technical Basis section to be included within the standard for clarifications of the following…" ***Who is the vendor? Is it the manufacturer/software company, the reseller the hardware/software is acquired from, the shipping company, the integrator, others? For temporary staff, is the contract employee a vendor?***"

Likes 0	
Dislikes 0	

Response

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

The intent of FERC Order 829 is noble, but seems to be directed to the wrong audience. The risks of compromised hardware and software impacts much more than ICS, in that it extends to all our processing and communication systems. With the advancement of IoT, the spirit of FERC Order 829 needs to be moved to an even higher national focus. In the meantime, NERC should focus on helping registered entities improve its controls culture within the activity environment it can directly impact. Thanks.

Likes 0	
Dislikes 0	

Response

Devin Elverdi - Colorado Springs Utilities - 1

Answer	
Document Name	

Comment

Refer to CSU comments.

Likes 0	
Dislikes 0	

Response

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Response	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	
Document Name	
Comment	
By not modifying the existing CIP Standards where there is overlap of requirement, there is a distinct possibility of inconsistent policies and procedures. Furthermore, should the Registered Entity choose to reference its other Standards compliance documents, there is a possibility of creating circular references or “spaghetti” linkages.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	
Document Name	
Comment	
Avista commends the SDT and NERC for the extensive work done on developing this standard. Avista also supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Response	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	
Document Name	
Comment	

1) Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

2) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

3) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

4) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

b. Move CIP-013 R3, to CIP-010 R1.

c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

d. Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	
Response	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	
Document Name	
Comment	

This Standard implies a high degree of compliance audit and enforcement authority for the Regions, which we have not seen implemented. From our experience with CIPv5 compliance exceptions, the objectives of the Reliability Assurance Initiative to provide risk-based process efficiencies have not been met. Entities must still use the costly self-report process for anything short of perfection, and regional auditors are not given latitude to make risk-based decisions. CIP-013-1 as drafted cannot work as intended until entities can work with regional auditors to quickly assess risk.

Likes 0	
Dislikes 0	

Response

George Tatar - Black Hills Corporation - 5

Answer	
Document Name	

Comment

See Black Hills Corp comments

Likes 0	
Dislikes 0	

Response

Wes Wingen - Black Hills Corporation - 1

Answer	
Document Name	

Comment

The intent of FERC Order 829 is good, but seems to be directed to the wrong audience. The risks of compromised hardware and software impacts much more than ICS, but extends to all our processing and communication systems. With the advancement of IoT, the spirit of FERC Order 829 needs to be moved to an even higher national focus. In the meantime, NERC should focus on helping registered entities improve its controls culture within the activity environment it can directly impact. Thanks.

Likes 0	
Dislikes 0	

Response

Jamie Monette - Allete - Minnesota Power, Inc. - 1

Answer	
Document Name	

Comment
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.

Likes 0	
Dislikes 0	

Response

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb

Answer	
Document Name	

Comment
Note of Appreciation We recognize the constraints imposed on the Standard drafting process by the language of the Commission's Order and its directives. We also would highlight Commissioner LaFleur's caution--that the Order was premature—may be coming to fruition. In consideration of both points, we are appreciative of the Standard Drafting Team's continuing work on the CIP Cyber Supply Chain Standard and its efforts to overcome the challenges it presents. Thank you. Kansas City Power and Light Company

Likes 0	
Dislikes 0	

Response

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	
Document Name	

Comment
Oxy supports the comments of MRO.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	
Document Name	
Comment	
The current version of CIP-013-1 is vague. Though flexibility is needed, the current version does not provide enough clarification to Registered Entities on the expectations required under the Standard and will therefore fail to mitigate cyber security risks to the BES.	
Likes 0	
Dislikes 0	
Response	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	
Document Name	
Comment	
We have several questions and concerns about what the phrases "vendor-initiated" and "system-to-system remote access" used in several requirements exactly mean. 1) Can the SDT please clarify what is meant by “vendor-initiated”. For example, if we (the customer) are having an operational issue and contact the vendor for support, is that support session still considered “vendor-initiated”, or would that session not be in scope because it is prompted by the customer’s request? Alternatively, if we initiate the remote access session with the vendor and turn over control to them, is that session still considered "vendor-initiated"? 2) We are unclear what the phrase "system-to-system" means. Please define or give examples of what would be considered a “system-to-system remote access with a vendor”. We are having trouble understanding how we might apply R4.1-4.3 and other associated requirements if there is no human interaction. 3) In our experience, vendor or third-party remote assistance is typically needed in times where there is a problem that could not be resolved by internal staff. We are concerned with the monitoring requirement (4.2), especially in situations where the system issue is having a real-time impact on operations and requires speedy trouble-shooting and resolution. There may not be enough internal resources available to respond to the situation and also actively monitor the vendor’s session. Additionally, the use of the phrase “unauthorized activity” is problematic, as the situation may not allow for a step-by-step explanation from the vendor as to what steps they are taking to troubleshoot the issue. Finally, how would one prove in an audit that the session was monitored and that no unauthorized activity occurred? Tri-State strongly believes the directives issued in Order No. 829 should be addressed by revising existing CIP standards, so that entities have all the relevant requirements together. We are concerned that if the existing standards are not revised to incorporate the new requirements, we will recreate the confusion and complexity that came with v3 standards, which in many cases led to non-compliance. We encourage NERC to request more time from FERC to get this right the first time and to avoid future projects, if extra time is needed, and instead allow the industry to focus more time and resources on getting cyber security right.	
Likes 0	
Dislikes 0	
Response	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	
Document Name	
Comment	
Concur with EEI’s Position	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	
Document Name	
Comment	
- See APPA's comments.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA thanks the SDT for its work on this challenging project in such a short amount of time.	
Likes 0	
Dislikes 0	
Response	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	
Document Name	

Comment
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	
Document Name	

Comment
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant

Answer	
Document Name	

Comment
We appreciate the hard work of the standard drafting team in putting together this first draft standard and supporting documents. This is a very different type of standard than usual that asks entities to address risks that may be introduced by activities outside of their control. Although we have concerns with this first draft, we feel confident that the team can work through the issues and come up with a reasonable set of requirements. If low impact Cyber Systems are included in any of the requirements, the requirements should be less stringent than those for high and medium since the risk to the BES is considerably less. Some of the other CIP standards use applicability tables to more clearly illustrate the specific requirements for

each of these impact levels (see CIP-004 for an example). If there are any variations in requirements for the impact levels – especially if low impacts are included in this standard - we would like to see the tables used. They provide consistency with the way the other standards are written, they're easier to navigate, and they can illustrate the risk-based nature of the standard.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.	
Likes 0	
Dislikes 0	
Response	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	
Document Name	
Comment	
Support EEI comments.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	

Document Name	

Comment

The drafting team should consider addressing some sort of vendor certification process to enable entities to select vendors that meet all of the security requirements stated within this standard. This will enable entities to rely on these vendors while allowing the entity to expeditiously address security vulnerabilities and other risks to operations.

Likes 0	
Dislikes 0	

Response

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	
Document Name	

Comment

At the outset, Southern Company wishes to first note for the record its belief that Requirement R3 and Requirement R4 should be removed from the CIP-013 standard. As explained below, it is either duplicative of R1, duplicative of existing requirements in CIP-004-6, CIP-005-5, CIP-007-6, CIP-008-5, and CIP-010-2, and is inappropriate for a standard focused on the Supply Chain time horizon.

First, from the perspective of a supply chain procurement time horizon, verification of the integrity and authenticity of software and firmware is already addressed under Requirement R1, R1.2.3. Specifically, R1 requires a risk management plan that addresses controls for mitigating cybersecurity risks for industrial control system vendor products and services, and the plan must address methods to evaluate controls to address those risks (R 1.2) including “process(es) for verifying software integrity and authenticity of all software and patches that are intended for use”. (R 1.2.3) Specifically, (assuming R1 covers only the procurement time horizon), then R3’s requirement -- to implement “one or more documented processes” to address the verification of the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems -- is arguably covered by R1.2.3’s requirement to have a process to do the same with respect to all industrial control system software and patches.

Second, to the extent R1 or R3 could be read to extend to verification of authenticity/integrity beyond the procurement and into the operational phase, such a broad interpretation should be outside of the scope of the CIP-013 supply chain standard, and would be more appropriately addressed in a separate proceeding to look specifically at operational standards CIP-002 through CIP-010. Specifically, patch monitoring and management is already described in CIP-007, yet little consideration appears to have been given to the burdensome impacts that might result on CIP-007 compliance if CIP-013 R3 compliance is layered on top in the operational time horizon, rather than being limited to the procurement phase (and thus covered in CIP-013 R1). The stringent 35 day cycles required within CIP-007-6 R2 will be significantly impacted by the proposed language in R3, placing Responsible Entities in a position of compromising compliance with one standard by trying to maintain compliance with another. The supply chain NOPR and final were not originally focused on these types of operational controls, and any such exploration of operational risk issues are more appropriately explored separately and outside of the supply chain proceeding. Moreover, if this standard is intended to cover all aspects of all lifecycle stages (from planning to procurement to production to retirement, i.e., cradle to grave) for all devices and vendors – that is an expansive initiative that overlaps with multiple CIP standards and would require a timeframe for development that is much longer than one year.

Similarly and for the above reasons, Requirement R4 is also considered not necessary and should be removed. The proposed requirement for "authorization of vendor remote access" is already explicitly required in CIP-004-6 R4; logging and monitoring of vendor remote access is already covered in CIP-005-5 R1 and CIP-007-6 R4; and response to "unauthorized activity" by vendors is already covered in CIP-008-5. The modifications provided above and suggested under R4 are to address the Responsible Entity having the capability to quickly disable vendor remote access sessions, which again we strongly recommend the SDT consider incorporating into CIP-005 as a new requirement addressing this potential security improvement.

Overall, industry was not given an adequate chance to express this in the FERC proceeding leading to Order 829 because the NOPR expressed proposed directives at a very broad and high level whereas the Final Rule contained much more prescriptive directives. Southern Company agrees with the July 21, 2016 statement provided by Acting Chairman LaFleur in this proceeding that "the more prudent course of action" for NERC, industry, and stakeholders would have been to issue a supplemental NOPR to provide input on the more prescriptive directives contained in this Final Rule. Southern Company would encourage an opportunity for input on such larger matters once the standard is submitted to the Commission for approval. Having said that, Southern Company recognizes and appreciates that, at this stage of standard development, NERC is bound to comply with the final rule's directives in Order 829. Therefore, while wishing to preserve for the record its opinion that Requirement R3 and R4 should be removed, Southern Company offers the comments and language contained herein to improve the standard from its currently drafted version.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	
Document Name	

Comment

ITC agrees with the comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Dennis Sismaet - Northern California Power Agency - 6

Answer	
Document Name	

Comment

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	

Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	Project 2016_03_ Exelon Comments_ 030617.docx
Comment	
Likes 0	
Dislikes 0	
Response	

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Risk Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on proposed **CIP-013-1 – Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing 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 Bulk Electric System (BES) operations as follows:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

Questions

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

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you

agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No

Comments:
The draft Requirement R1.2 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R1.2, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless a vendor agrees to notify the Responsible Entity of vendor-identified vulnerabilities in the Cyber Assets provided or maintained by the vendor, Responsible Entities cannot comply with R1.2.3.

Responsible Entities could encounter scenarios where:

- Vendors may refuse to comply with the Responsible Entity's vendor controls;
- Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;
- Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or
- Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's required controls. Such a "safety valve" would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Guidance language in the G&TB portion of a Standard is helpful, but the "safety valve" concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary "safety valve" along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply

chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Exelon feels that the R2.1 language is vague and has the potential to become administratively burdensome without a corresponding benefit to BES reliability. While Exelon agrees with the rationale that examples of sources of information that an entity could consider include guidance or information issued by the E-ISAC, this language should be included in the Requirement itself because only that language forms the basis of a compliance assessment. Exelon receives over 100 security-related messages regarding potential vulnerabilities per day from a myriad of sources. Without creating bounds around the sources to be considered as well as the periodicity for updates to supply chain cyber security risk management plan(s), the question of whether any or all of the messages should have been considered will be difficult, if not impossible, to evidence. Exelon points out that the E-ISAC already performs important filtering functions for the industry. Perhaps future Alerts issued by the E-ISAC could be enhanced to point out vulnerabilities that would require new mitigating controls in supply chain cyber security risk management plan(s). Without these limitations, each entity will need to develop processes and procedures to receive and filter information, define mitigating controls, update the plan(s) and obtain approvals which is inefficient at best and impossible to evidence at worst.

Further, Exelon suggests that while multiple updates to the plan(s) may occur within a year as new E-ISAC Alerts are issued, CIP Senior Manager Review and Approval should only be required every 15 months. Intermediate reviews and approvals, or reviews for minor changes, should be outside the scope of the Requirement.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

The draft Requirement R3 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R3 compliance, particularly in circumstances where only a single vendor has the capability of

providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless the vendor agrees to cooperate with any software integrity and authenticity verification process, the Responsible Entity will be unable to ensure the integrity and authenticity of software used in covered Cyber Assets.

Responsible Entities could encounter scenarios where:

- Vendors may refuse to comply with the Responsible Entity's vendor controls;
- Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;
- Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or
- Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's required controls. Such a "safety valve" would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Guidance language in the G&TB portion of a Standard is helpful, but the "safety valve" concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary "safety valve" along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

Exelon does not support the draft language in R3 which requires an Entity to verify the integrity and authenticity before placing a BES Cyber System into operation. Instead, Exelon prefers the suggested language from Order No. 829 that directs "the integrity of the software and patches before they are installed in the BES Cyber System environment" (P. 48). Accordingly, Exelon suggests that R3 be edited to read as follows:

Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware **prior to installation into** high and medium impact BES Cyber Systems

In addition, see the concerns under (4) below regarding potential overlap between R3 and existing CIP Standards.

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

The proposed Requirement creates significant overlap with existing CIP Requirements. Requirement R4, as well as Requirements R3 and R5, should be modified so that CIP-013 only addresses those aspects of software integrity and authenticity (R3), remote access (R4), and authenticity and remote access for low impact BES Cyber Systems (R5) not covered by other Standards. Exelon understands that the timeframe dictated by FERC in Order No. 829 does not allow for revisions by this SDT to the relevant Standards that address these topics. However, overlap between the Standards should be avoided as much as possible to avoid double jeopardy concerns in the event of potential non-compliance with CIP-013 R3, R4, and R5.

For example, Exelon's review of the draft CIP-013-1 Standard indicates the following areas of overlap:

- CIP-013-1 R3.1 through R3.4 require authentication of operating systems, firmware, software, and patches. However, the configuration change management requirements under CIP-010-2 R1 already require that the configuration of operating systems, firmware, and software be carefully tracked such that counterfeit operating systems, firmware, software, and patches would be identified (e.g. a software difference would be identified as a change from the existing baseline configuration) and would be evaluated.
- CIP-013-1 R3.4 requires authentication of patches, updates, and upgrades, but CIP-007-6 R2.1 already imposes a patch management process for tracking, evaluating, and installing cyber security patches, including the identification of patching sources. Part of the identification of patching sources under CIP-007-6 is the verification that those sources are authentic as CIP-013-1 R3.4 would appear to require.
- CIP-013-1 R4.1 requires authorization of remote access to certain BES Cyber Systems by the vendor. CIP-004-5 R4.1.1 already contains a process for authorizing electronic access to these assets by all personnel, including vendors.
- CIP-013-1 R4.2 requires logging and monitoring or remote access sessions. CIP-007-6 R4.1 already requires logging of all access and CIP-007-6 R4.2 requires alerting for any malicious code as well as any "security ecent that the Responsible Entity determines necessitates an alert."
- CIP-013-1 R4.3 also requires responding to detected unauthorized activity, and because unauthorized activity on a BES Cyber System would constitute a "Cyber Security Incident," CIP-008-5 already requires a response to such incidents.

- CIP-013-1 R5 requires a process for controlling vendor remote access to low impact BES Cyber Systems. This overlaps with CIP-003-6 Attachment 1 Section 3 which already requires electronic access controls for low impact BES Cyber Systems the limit access to necessary access.

The draft CIP-013-1 requirements should be modified so that overlaps are removed and that CIP-013-1 only addresses vendor issues not covered within existing Standards. To the extent the SDT believes there is no overlap between CIP-013 and the existing CIP Standards, the SDT should explain in each instance where the CIP-013 Requirement ends and the other CIP Requirement begins. In the absence of such guidance, a Compliance Monitoring and Enforcement Process could conclude that a particular instance of non-compliance with CIP-013 is also a simultaneous violation of another Reliability Standard, doubling the available penalty range. For example, draft CIP-013-1 R4 requires the Responsible Entity to authorize remote access by vendor personnel. The current CIP-004-6 R4.1.1 also requires authorization of vendor personnel to have electronic access. Therefore noncompliance with CIP-013-1 R4 would appear to, per se, constitute noncompliance with CIP-004-6 R4.1.1. Such double jeopardy serves no apparent reliability purpose. If the current CIP-013-1 R4 language is adopted as-is, the SDT should explain how its requirements differ from those under CIP-004-6 R4.1.1.

Finally, Exelon suggests that R4.3 may be difficult to accomplish in all cases and is overly prescriptive and thus should be removed from CIP-013. Order No. 829, P.52 references the Ukraine event and 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." There are alternate methods to address this threat. First, two factor identification methods can be used to mitigate the risk of stolen credentials. Second, the use of WebEx or Skype sessions or active control of vendor access (i.e. opening a port for access only when needed) can be used to address emergent issues and reduce the need for remote persistent sessions.

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Exelon has the same concerns regarding the lack of a compliance "safety valve", the potential for double jeopardy as well as the administrative burden of updating the supply chain cyber security risk management plan(s) for newly identified vulnerabilities as included in the comments on R1-R4. The discussion under (4) identifies how the proposed R5 overlaps with existing CIP Standards.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

☒ Yes
☐ No
Comments:

Exelon generally agrees with the Implementation Plan for CIP-013-1 but offers the following recommendation for clarifying the plan for R2.

The initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 must be completed within fifteen (15) calendar months **following** the effective date of CIP-013-1. There should be no obligation to review the plans ahead of time, and only the initial development and implementation should be required. This should be made clear in the Implementation Plan.

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

☐ Yes
☒ No
Comments:

On Page 9, line 43, the Technical Guidance and Examples references the use of industry best practices and guidance that improve cyber security risk management controls. This does not match the rationale of R2 which only speaks to the use of guidance. Exelon feels that the reference to "industry best practices" should be removed from the Technical Guidance and Examples since it is non-specific and open to interpretation.

9. Provide any additional comments for the SDT to consider, if desired.

Comments:

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Risk Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on proposed **CIP-013-1 – Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing 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 Bulk Electric System (BES) operations as follows:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

Questions

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

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you

agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

ERCOT supports the IRC comments and offers the following supplemental comments.

FERC Order 829, Paragraph 59, states that NERC's new or modified 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." This does not include the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) listed in R1. These systems do not perform or provide bulk electric system operations. ERCOT believes the inclusion of these systems in the draft standard goes beyond the scope of the standard intended by FERC and recommends the SDT remove them from the applicable systems of the standard language.

Requirement R1 requires Responsible Entities to have a plan that addresses processes for notification of a vendor's cyber security events (R1.2.1) and vulnerabilities (R1.2.3), as well as coordination of cyber security incident response activities (R1.2.4). As this information is highly sensitive, it is unlikely that all vendors will agree in all cases to provide this information unless they are already required to do so under other regulatory obligations. Responsible Entities cannot force a vendor to agree to these terms, and in cases where the vendor deems the risk of this disclosure too great compared to the value of the contract, the vendor will decline to enter into the agreement. This will force the Responsible Entity to seek another vendor that is willing to accept these terms, and such a vendor may or may not exist. Because it is possible that a Responsible Entity may be unable to identify a vendor that is willing to accept a contract with the terms required by R1, the proposed standard could seriously hamper the essential functions of Responsible Entities. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R1. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Requirement R1.2.2 requires "notification when vendor employee remote or onsite access should no longer be granted." The revocation of access, including Interactive Remote Access, is currently addressed in CIP-004, R5. Since the background checks, training, access authorization, and access revocation for employees and vendors is already addressed in CIP-004, the drafting team should ensure any new requirements related to access revocation of vendors be placed in CIP-004. In developing the CIP Version 5 standards, extensive work was undertaken to ensure that all requirements related to the subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework.

Requirement R1.2.5, which requires a Responsible Entity's plan to include "Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use," is duplicative of Requirements R3 and R5 within this standard, which also require documentation of processes. ERCOT recommends removing R1.2.5.

Requirement R1.2.6 requires an entity's plan to include "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)." This requirement is duplicative of Requirement 4 within this standard. ERCOT recommends removing Requirement R1.2.6, which also requires documentation of processes.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☒ Yes
☐ No
Comments: ERCOT supports the IRC comments on this question.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

ERCOT supports the IRC comments on this question and offers the following supplemental comments.

ERCOT recognizes the need for the concepts contained in Requirement R3. However, ERCOT disagrees with the placement of the requirement in a new standard. Since this requirement is applicable to only high and medium impact BES Cyber Systems, it should be placed within CIP-010. The requirement directly impacts the baselines that have been established within CIP-010 R1. The SDT could insert a new part between existing Parts 1.1 and 1.2 in that standard. The new part could use the following language: "For any updates or patches that that deviate from the existing baseline configuration, verify the authenticity and integrity of the update or patch." As mentioned previously, in developing the CIP Version 5 standards, the SDT performed extensive work to ensure that all requirements related to a particular subject were included in one standard instead of being spread across multiple standards. The proposed language will

disrupt that framework. Including the requirement in CIP-010 will ensure that a single standard captures all parts of the change process, including inventory (Part 1.1), validation of the code (NEW), authorization of implementation (Part 1.2), update of the inventory (Part 1.3), and testing of the change (Parts 1.4 and 1.5). This approach would give Responsible Entities a complete view of what is required from the start to the end of a change. It also prevents entities from keeping separate inventories to meet the CIP-010 requirement and the CIP-013 requirement.

Additionally, ERCOT requests guidance on how to demonstrate compliance when using automated solutions to obtain the most current patches applicable to their systems. In large environments, these automated solutions are critical to meeting the timing obligations of CIP-007 R2. Inserting the manual step of verifying integrity and authenticity of updates and patches can prevent the use of these solutions that entities have invested in and rely upon for addressing security risks and regulatory obligations. If it is intended that the entity may simply document the source used by these solutions, it would be helpful to put such clarifying language in the requirement.

Additional use cases for the SDT to consider in developing guidance include: (1) how signature and pattern updates are contemplated within the requirement since these are not updates to the operating system, software, or firmware noted, (2) instances when code is packaged and mailed to an entity, (3) software and firmware that are part of a vendor black-box type of appliance solution where the entity has no visibility to the code on the device, and (4) vendors bringing code onsite that the entity is not allowed to review. Any of these cases could present an obstacle to strict compliance with the draft standard language.

As with Requirement R1, this requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. The drafting team should address situations in which vendors will not or cannot provided the levels of service mandated by this requirement. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R3. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

ERCOT supports the IRC comments and offers the following supplemental comments.

Requirement R4 is duplicative of existing requirements in CIP-004, CIP-005, CIP-007, and CIP-008. The drafting team should consider modifications to these existing standards rather than creating new requirements in a new standard. By placing these requirements in a stand-alone Standard, there is a possibility that entities may not make necessary connections to the prerequisites of some requirements (e.g., CIP-004 R2, R3) and downstream obligations of other requirements (e.g., CIP-008). ERCOT offers the following suggestions for realignment:

Requirements for electronic access authorization of vendors, including Interactive Remote Access, are addressed within CIP-004 R4, which also addresses the proper vetting and training of said vendors. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper pre-authorization requirements.

Requirements for Interactive Remote Access are already addressed within CIP-005 R2. Vendor-initiated remote access is just one example of Interactive Remote Access. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper configuration of remote access (e.g. multi-factor authentication, encryption, Intermediate System).

Requirements for system-to-system communications are already addressed within CIP-005 R1. This requirement could be added to CIP-005 R1 or as an addition to R2. The heading for Table 2 within CIP-005 can be modified to “Remote Access” in support of this. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper network controls for the system-to-system communication (e.g. ESPs, EAPs, etc.).

Requirements for logging and monitoring of access activity are addressed in CIP-007 R4. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify the logging specifications that differ from CIP-007 R4.

Requirements for response to unauthorized activity are already addressed within CIP-008. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify integration with CIP-008.

There are also several instances in the standard where language needs to be clarified. The drafting team should state whether system-to-system remote access includes “phone home” capabilities that are used for reporting of licensing, system health, and system problems. Requirement R4.1 should be clarified to specify whether it is addressing authorization of each remote access session or remote access to the vendor in whole. The drafting team should consider whether this requirement is consistent with current requirements in CIP-004 R4. The drafting team also needs to address authorization of software companies that use a “follow-the-sun” support model. Follow-the-sun is a type of global support where

issues are passed around daily between work sites that are many time zones apart. Such a support increases responsiveness.

As noted with other requirements in the draft CIP-013 standard, the drafting team should address situations in which vendors will not or cannot provide the levels of service mandated by this requirement. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling to agree. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R4. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

As with other comments, this requirement is duplicative and should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to refer to a single standard to for security plan requirements.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Twelve months is not sufficient time to allow compliance with all aspects of this standard. The drafting team should consider a phased approach allowing the logical phased implementation of these requirements.

While the Implementation Plan suggests that existing contracts need not be modified, the proposed standard language does not make this clear. ERCOT believes the standard to be a more appropriate

location for this exemption, as it is ultimately substantive in nature. ERCOT there recommends that the drafting team include language in the standard explicitly limiting applicability of the requirements to new contracts.

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

☒ Yes
☐ No
Comments: No comments

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

☐ Yes
☒ No
Comments:

Although NERC's Compliance Guidance Policy document describes certain procedures by which a drafting team may provide Compliance Guidance, ERCOT suggests that it is generally preferable to provide examples of acceptable conduct in the standard itself, rather than in an ancillary document, which Responsible Entities would have to remember and separately locate and review. The team could achieve this purpose by using language in the standard such as: "Practices that comply with this requirement include, without limitation, the following: . . . ." ERCOT notes that in a number of instances, the draft Technical Guidance and Examples document uses normative language (e.g., "should"), rather than permissive (e.g., "may") language, which suggests that the Technical Guidance document is instead intended to serve simply as a more detailed set of requirements, as opposed to describing one of potentially many acceptable methods of achieving compliance. For example, the guidance for R1 states: "In implementing Requirement R1, the responsible entity should consider the following: . . . ." To the extent the drafting team intends the guidance in this document to be followed, it should be included in the standard.

9. Provide any additional comments for the SDT to consider, if desired.
Comments:
The drafting team should consider addressing some sort of vendor certification process to enable entities to select vendors that meet all of the security requirements stated within this standard. This will enable entities to rely on these vendors while allowing the entity to expeditiously address security vulnerabilities and other risks to operations.

Foundation for Resilient Societies Comments on Draft Standard 2016-03, Cyber Security Supply Chain Risk Management, NERC CIP 013-01

1. Vote "NO" on approval of the draft.

   Rationale: The proposed CIP-013-01 standard is onerous and not cost-effective. It excpectss too much of individual registered entities, which should not be the primary organizations responsible for strengthening the integrity of the cyber supply chain.

   Starting at the foundry level, it is essential to assure the integrity of chip design, manufacture and operations. And control of firmware by entities that are committed to protect the national security interests of the United States and Canada. The current practice of purchasing control and telecommunication systems from the lowest-cost supplier may be too risky and too imprudent to attain greater integrity in cyber supply chains. It is unreasonable to expect that some 1400 separate electric utilities should be responsible for major changes in the development and regulation of cyber supply chain systems.

   The recent re;port on Cyber Deterrence by the Defense Science Board, released on February 28, 2017, seeks tailored initiatives to enhance deterrence of cyber attacks on critical infrastructures. This Report recognizes that a key element of deterrence is to improve defenses, so the payoffs to foreign adversaries will be reduced. Meanwhile, the Trump Administration has underway a review of cyber policies and strategy. If the Administration will support initiatives to strengthen cyber supply chains that involve indigenous U.S. design, production, operation, and integrity testing for the entire cyber supply chain, any final NERC-FERC standard responsive to Order No. 829 should await opportunities to be presented by the Administration after its policy review.

   As a result of this overburden on registered entities, the Standard Drafting team -- not surprisingly -- has drafted CIP-013-1 containing too many exceptions, qualifications, and outstanding conflicts to form the foundation for the most-difficult process of managing the risks that derive from vulnerabilities in products marketed to the industry in a global and highly competitive environment. If some foreign governments subsidize their hardware systems, is it imprudent to always accept the lowest price products that place our cyber supply chains at risk?

   The present draft standard makes the probability of successful discrimination exceedingly low. The investment of time and money by utilities and the industry will be very high, and certainly not worth the risks of failing compliance by entities and their procurement selections that are even further removed from technical competencies essential to their task.

   Implementation as written will only encourage a shell game that will delay real solutions to the Supply Chain vulnerabilities and provide false assurances that must be addressed collectively by the industry, by state and by federal authorities. The latter must address the increasing failures of vendors to design secure products through market motivations and penalties. This problem has been successfully addressed in many other industries where serious safety issues existed.

2. **Requirement R1**
   a. Any deep examination of the four objectives of R1 reveals substantial gulfs with the realities of Supply Chain issues.

- Risks can never be assessed in the absence of vulnerability assessments. None are called for. And vulnerabilities range from individual components to full systems. End-to-end control center to remote unit network assessments are needed.
- A component flaw might trace to a vendor several stages removed from the utility and vulnerabilities are often the product of several vendors' missteps.
- Adversarial efforts impact multiple systems and subsystems; hardware and software and firmware, classical attack vectors and subtleties difficult for even professional forensic experts. These challenges are beyond utilities' ability to assess.
- The "prior contract" exclusion leaves open vulnerabilities introduced post "contracting." Note that the February 2017 Defense Science Board Report on Cyber Deterrence calls for improvements in defensive capabilities as a key element of deterrence. The "prior contract" exception will assure access by foreign adversaries that will enable continuing implantation of malware, continuing exercise of equipment within the U.S. electric grid and within other critical infrastructures upon which the North American electgric grid depends. . These"prior contract" exceptions are inexcusable; a program needs to be developed -- not by individual registered entities -- to assist in the removal and replacement of hazardous hardware, firmware, and software.
- The absence of hard requirements for "secure vendor accesses", "Internet avoidance", "encryption", "blacklisting known malware", etc. reveals industry ambivalence re: enforceable supply chain controls.
- No plan can possibly be developed that will adequately cover the variety of situations and conditions that exist. They are far too complex to be "planned for" separately by over 1400 independent "Responsible Entities". And we observe the usual escape clause, ***"Obtaining specific controls in the negotiated contract may not be feasible and it is not considered failure to implement an entity's plan".*** How does one define ***success***, under these circumstances?

b. **Requirement R2**. The R2 process is clearly a bureaucratic device; an artificial deadline for updating the plan, get approval from the senior CIP manager (who should have sustained involvement, not at 15 month intervals.) If this process is adopted and approved, the net result will be to undermine the goal of cyber deterrence as enunciated in the February 2017 Defense Science Board Report. Intervals of 15 months between assessments and corrections will enable large gaps that foreign adversaries will exploit.

c. **Requirement R3.** Implementing one or more documented processes for verifying the integrity and authenticity (medium and high impact BES systems) for software and firmware would require substantial forensic competency by the utility. Further, in the reality of the sophisticated attacks that have given rise to Order No. 829, there is very little likelihood of success by over 1400 independent "responsible entities" and the potential for unreasonable expenses in the process. Or did the SDT intend to minimize

the task? This illusory requirement illustrates the need for broader initiatives, both within the electric utility industry and outside the industry.

d. **Requirement R4.** The requirement for controlling vendor remote access seriously ignores many gaps and related problems In CIP v5/v6, in the categorization structure and in the process proposed. It fails to lay down hard controls on vendor access and yet requires a complex "documented" process which can easily pass table top compliance review without correcting the many holes in systems as they operate that will remain available to adversaries. Exceptions to CIP standards leave thousands of cyber assets directly interfacing with the internet, not covered by this standard as well as all others. Yet those assets are directly linked to OT and IT systems providing paths for malware, data corruption and opportunities for adversarial control, through supply chain vulnerabilities. With respect to Supply Chain vulnerabilities, Grid connectivity makes nonsense of the categorization of Cyber Assets as "low", "medium" and "high" impact.

e. The practice of rating a low impact asset as "no effect on the BES overall" has consistently ignored the sum of such assets effect on the vulnerabilities of the Grid to uncontrled separation and cascading outages, and permanent damage to long-replacement-time grid equipment.

f. **Requirement R5**. Given the holes described in **R4**, this requirement for verifying product integrity and controlling vendor accesses, and presumably unmonitored machine-to-machine accesses for the few low impact cyber assets covered by CIP standards, is intended to obscure the realities of major portals available to the nation's adversaries. FERC knows CIP standards utterly fail to address the vulnerabilities of so-called low level , so-called "Low Impact" cyber assets, as have been demonstrated to enable takedown of elements of the Ukrainian electric distribution system in both December 2015 and December 2016 . FERC knows that such assets represent major avenues for attack on the BES and the short path to "Distribution" systems and nuclear sites. Notwithstanding, the current supply chain standard needs a major overhaul to provide effective and verifiable system security.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on proposed **CIP-013-1 – Cyber Security - Supply Chain Risk Management**. The electronic comment form must be completed by **8:00 p.m. Eastern, Monday, March 6, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing 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 Bulk Electric System (BES) operations as follows:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed proposed CIP-013-1 to address the above directives.

Questions

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

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you

agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:
Seattle City Light has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Seattle City Light does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, Seattle City Light requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Seattle City Light believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, Seattle City Light requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Seattle City Light requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

Seattle City Light is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. In some cases use of these contracts in procurement is mandated by other laws or regulations. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see Seattle City Light’s response to Question #9 for additional information on exceptions).

Seattle City Light notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 Seattle City Light requests changing the word *evaluate* to *determine.*

For R1.2.1 Seattle City Light requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 Seattle City Light requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. Seattle City Light requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

In Measure M1, Seattle City Light requests that the language be changed to be consistent with the Requirement. Specifically, change "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…" to "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…" (BOLD emphasis added). The construction "address risk" conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as alternatives to being mitigated.

Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☒ Yes
☐ No
Comments:

Seattle City Light agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Seattle City Light requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s)

specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Seattle City Light requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Seattle City Light requests changing the language to “upon detected unauthorized activity”.

Furthermore, because it may not be technically feasible to remotely disable a vendor from equipment provided by that vendor (which the entity purchased from them, and may be dependent upon the vendor for maintenance), Seattle City Light requests the inclusion of a Technical Feasibility Exception (TFE) for R4. Seattle City Light suggests the following language: "WHERE TECHNICALLY FEASIBLE, each responsible entity shall implement one or more documented process(es) for controlling vendor remote access to…" (emphasis added).

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Seattle City Light requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, Seattle City Light requests that all requirements related to low impact assets be included in CIP-003.

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Seattle City Light requests a 24-month implementation plan.

Seattle City Light requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

☐ Yes
☒ No
Comments:

Seattle City Light does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Seattle City Light requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Seattle City Light requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

☐ Yes
☒ No
Comments:

Seattle City Light requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging.

Seattle City Light requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

Seattle City Light requests clarification on the term "supplier" as it is used in the guidance document. Seattle City Light requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, Seattle City Light requests an explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

The Rationale sections of CIP-013 standard and the guidance document use the term "information system". Seattle City Light requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced Seattle City Light requests that the SDT define the term and place it in the NERC Glossary of Terms.

Seattle City Light requests that the SDT consider defining the term "Security Event" (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. Seattle City Light requests that the following language added to the definition "have potential adverse impacts to the availability or reliability of BES Cyber Systems" and that the entities be required to report only newly identified security vulnerabilities.

Additionally, Seattle City Light requests that the SDT define the term "vendor security event" or replace it with "identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System."

9. Provide any additional comments for the SDT to consider, if desired.
Comments:

Seattle City Light understands that the SDT is under time constraints in addressing Order No. 829, however, Seattle City Light requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Seattle City Light requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Seattle City Light feels that all standards with requirements that apply to low impact assets should be included in CIP-003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to Seattle City Light if this was intentional for R3 and R4. Seattle City Light requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

As discussed in comments to R1 above, Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.

Seattle City Light recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, City Light agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and City Light urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address the gaps that remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns. Thus this standard "does not advance the security of the grid," as set out by now-Chairperson LaFleur in her dissent to Order 829.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2016-03 Cyber Security Supply Chain Risk Management | CIP-013-1
Comment Period Start Date:	1/19/2017
Comment Period End Date:	3/6/2017
Associated Ballots:	2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 Non-binding Poll IN 1 NB

There were 134 sets of responses, including comments from approximately 231 different people from approximately 144 companies representing 10 of the Industry Segments as shown in the table on the following pages.

All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards Development, Steve Noess (via email) or at (404) 446-9691.

The Project 2016-03 Standards Drafting Team (SDT) appreciates the constructive feedback received from stakeholders during the initial posting of CIP-013-1. As a result of comments received, the SDT made significant revisions to proposed CIP-013-1 and developed revisions to other CIP standards as suggested by stakeholders. The three Reliability Standards now included in the project to address FERC Order No. 829 (CIP-013-1, CIP-005-6, and CIP-010-3) are being posted for 45-day formal comment period and will each undergo a 10-day ballot at the end of the comment period. Proposed Reliability Standards addressing the Order No. 829 directives must be filed for regulatory approval by September 27, 2017 to meet the filing deadline established by FERC.

Section 4.12 of the NERC Standard Processes Manual indicates that the SDT is not required to respond in writing to comments from the previous posting when it has identified the need to make significant changes to the standard, however the SDT is providing summary responses to the comments received in order to facilitate stakeholder understanding of the changes made for this posting.

The following is an overview of changes made by the SDT. Specific comments and revisions are discussed more fully in the summary consideration that follows.

- **Proposed Standards.** Project 2016-03 now encompasses three proposed standards in response to stakeholder feedback for better alignment with approved CIP standards:
  - **CIP-013-1 – Cyber Security – Supply Chain Risk Management**
  - **CIP-005-6 - Cyber Security – Electronic Security Perimeter(s)**
  - **CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments**

  Specific revisions were made in CIP-005-6 to address certain directives in Order No. 829 for controlling vendor remote access. Likewise, specific revisions were made in CIP-010-3 to address some directives in Order No. 829 for verifying software integrity and authenticity. Collectively the three proposed standards address the directives in Order No. 829.
- **Scope of BES Cyber Systems.** Requirements in proposed CIP-013-1 apply to high and medium impact BES Cyber Systems. The SDT removed low impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829.
- **Clarification of impact on existing contracts.** The SDT added a statement to the requirements section of CIP-013-1 to affirm that Responsible Entities are not required to renegotiate or abrogate existing contracts.

- **Clarification that Responsible Entities are not obligated for vendor contract terms and vendor performance.** The SDT added statements to the requirements section of CIP-013-1 to affirm that the actual terms and conditions of a procurement contract, and the vendor's performance under a contract, are not in scope of the proposed Reliability Standards.
- **Identifying and assessing cyber security risks in BES Cyber System planning.** The SDT revised CIP-013-1 Requirement R1 Part 1.1 to specify risks that Responsible Entities shall consider in planning for procurement of BES Cyber Systems.
- **Requirement to periodically review supply chain cyber security risk management plans.** The SDT clarified requirements for Responsible Entities to review supply chain cyber security risk management plans every 15 months and removed administrative or ambiguous parts.
- **Implementation Plan.** An Implementation Plan was developed to cover the three proposed standards. The proposed effective date for all requirements in Project 2016-03 is increased from 12 months to 18 months after regulatory approval.
- **Violation Severity Levels (VSLs).** CIP-013 VSLs are revised to better account for degrees of performance in response to stakeholder feedback.
- **Draft Implementation Guidance.** The SDT developed draft Implementation Guidance to provide considerations for implementing the requirements in CIP-013-1 and examples of approaches that Responsible Entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-1. The draft Implementation Guidance is intended to highlight some approaches that the SDT believes would be effective ways to be compliant with the standard, and will be submitted for ERO endorsement as described in NERC's Compliance Guidance Policy.

Questions

1. [Page 16] The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

2. [Page 158] The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

3. [Page 219] The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

4. [Page 305] The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

5. [Page 400] The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

6. [Page 479] Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

7. [Page 543] Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

8. [Page 604] The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

9. [Page 691] Provide any additional comments for the SDT to consider, if desired.

The Industry Segments are:

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE

Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Chris Gowder	Chris Gowder		FRCC	FMPA	Tim Beyrle	City of New Smyrna Beach	4	FRCC
					Jim Howard	Lakeland Electric	5	FRCC
					Lynne Mila	City of Clewiston	4	FRCC
					Javier Cisneros	Fort Pierce Utility Authority	3	FRCC
					Randy Hahn	Ocala Utility Services	3	FRCC
					Don Cuevas	Beaches Energy Services	1	FRCC

					Jeffrey Partington	Keys Energy Services	4	FRCC
					Tom Reedy	Florida Municipal Power Pool	6	FRCC
					Steve Lancaster	Beaches Energy Services	3	FRCC
					Mike Blough	Kissimmee Utility Authority	5	FRCC
					Mark Brown	City of Winter Park	4	FRCC
					Chris Adkins	City of Leesburg	3	FRCC
					Ginny Beigel	City of Vero Beach	9	FRCC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC

					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Joe McClung	Joe McClung		FRCC	JEA Voters	Ted Hobson	JEA	1	FRCC
					Garry Baker	JEA	3	FRCC
					John Babik	JEA	5	FRCC
MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter	4		MRO NSRF	Joseph DePoorter	MGE	1,2,3,4,5,6	MRO
					Joseph DePoorter	MGE	1,2,3,4,5,6	MRO
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC

					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
DTE Energy - Detroit Edison Company	Karie Barczak	3		DTE Energy - DTE Electric	Jeffrey Depriest	DTE Energy - DTE Electric	5	RF
					Daniel Herring	DTE Energy - DTE Electric	4	RF
					Karie Barczak	DTE Energy - DTE Electric	3	RF
Con Ed - Consolidated Edison Co. of New York	Kelly Silver	1	NPCC	Con Edison	Kelly Silver	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange and Rockland Utilities	NA - Not Applicable	NPCC
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC
					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation	6	SERC

						and Energy Marketing		
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion and NextEra	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC
					Alan Adamson	New York State Reliability Council	7	NPCC

Edward Bedder	Orange & Rockland Utilities	1	NPCC
David Burke	UI	3	NPCC
Michele Tondalo	UI	1	NPCC
Sylvain Clermont	Hydro Quebec	1	NPCC
Si Truc Phan	Hydro Quebec	2	NPCC
Helen Lainis	IESO	2	NPCC
Laura Mcleod	NB Power	1	NPCC
MIchael Forte	Con Edison	1	NPCC
Kelly Silver	Con Edison	3	NPCC
Peter Yost	Con Edison	4	NPCC
Brian O'Boyle	Con Edison	5	NPCC
Greg Campoli	NY-ISO	2	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
Michael Schiavone	National Grid	1	NPCC
Michael Jones	National Grid	3	NPCC
David Ramkalawan	Ontario Power	5	NPCC

						Generation Inc.		
					Quintin Lee	Eversource Energy	1	NPCC
Colorado Springs Utilities	Shannon Fair	6		Colorado Springs Utilities	Kaleb Brimhall	Colorado Springs Utilities	5	WECC
					Charlie Morgan	Colorado Springs Utilities	3	WECC
					Shawna Speer	Colorado Springs Utilities	1	WECC
					Shannon Fair	Colorado Springs Utilities	6	WECC
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Louis Guidry	Cleco Corporation	1,3,5,6	SPP RE
					Robert Gray	Board of Public Utilities,KS (BPU)	3	SPP RE
					Shawn Eck	Empire District	1,3,5	SPP RE

						Electric Company		
Santee Cooper	Shawn Abrams	1		Santee Cooper	Tom Abrams	Santee Cooper	1	SERC
					Rene' Free	Santee Cooper	1	SERC
					Bob Rhett	Santee Cooper	5	SERC
					Chris Jimenez	Santee Cooper	1	SERC
					Troy Lee	Santee Cooper	1	SERC
					Glenn Stephens	Santee Cooper	1	SERC
PPL NERC Registered Affiliates	Shelby Wade	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Charlie Freibert	LG&E and KU Energy, LLC	3	SERC
					Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Dan Wilson	LG&E and KU Energy, LLC	5	SERC
					Linn Oelker	LG&E and KU Energy, LLC	6	SERC
Public Service	Sheranee Nedd	1,3,5,6	NPCC,RF	PSEG REs	Tim Kucey	PSEG - PSEG Fossil LLC	5	RF

Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC					Karla Jara	PSEG Energy Resources and Trade LLC	6	RF
					Jeffrey Mueller	PSEG - Public Service Electric and Gas Co	3	RF
					Joseph Smith	PSEG - Public Service Electric and Gas Co	1	RF
Midcontinent ISO, Inc.	Terry BIlke	2		IRC-SRC	Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. The SDT developed CIP-013-1 Requirement R1 to address the Order No. 829 directive for entities to implement a plan(s) that includes security controls for cyber security supply chain risk management of industrial control system hardware, software, and services associated with BES operations (P 43, 45). This plan(s) is intended to cover the procurement aspects of all four objectives in the order (P 34 - 62). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Summary Consideration: The SDT thanks all commenters. The SDT has revised Requirement R1 and the accompanying rationale section in response to stakeholder comments.

Specific comments and SDT responses are provided below:

Commenters stated that the scope of cyber systems covered by the requirement was too broad. Commenters stated Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) were not part of Order No. 829. The SDT has revised Requirement R1 to apply to high and medium BES Cyber Systems; the SDT believes entities should have the flexibility to determine the extent to which it must address supply chain risks to the associated cyber systems.

Commenters stated that low impact BES Cyber Systems should not be included in CIP-013. Some commenters did not believe there was sufficient reliability benefit to including low impact BES cyber systems; other commenters stated that any requirements for low impact BES Cyber Systems should be added in CIP-003. The SDT has removed low impact BES Cyber Systems from applicability of CIP-013-1 and is not proposing any new requirements to address cyber security supply chain risks for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829.

Commenters indicated that the scope of cyber security risks being addressed in R1 is unclear. The SDT removed unnecessary and unclear wording from Requirement R1 main requirement and revised Requirement R1 Part 1.1 to clarify the supply chain cyber security risks that must be addressed by the Responsible Entity in planning for the procurement of BES Cyber Systems.

Commenters recommended including rationale statements pertaining to impact of CIP-013 on existing contracts in the requirement. The SDT added a statement to the requirements section of CIP-013-1 to affirm that Responsible Entities are not required to renegotiate or abrogate existing contracts.

Commenters expressed concern that Responsible Entities would not be able to comply with the standard without vendor cooperation, or that vendor breach of contract would result in Responsible Entity noncompliance with CIP-013. The SDT added statements to the requirements section of CIP-013-1 to affirm that the actual terms and conditions of a procurement contract, and the vendor's performance under a contract, are not in scope of the proposed Reliability Standards.

Commenters suggested clarifications to the list of procurement topics in Part 1.2. The SDT revised the list to address stakeholder concerns.

Commenters recommended separating obligations to develop the supply chain cyber security risk management plans from obligations to implement the plans. The SDT revised CIP-013-1, adding a standalone requirement R2 for implementing plans developed in R1.

Commenters stated that *vendor* should be a NERC defined term for clarity. The SDT believes that the revised requirements and rationale in the second draft of CIP-013 address stakeholder concerns with clarity and scope. The SDT is not proposing a formal definition for vendor because a one-size-fits-all definition could limit entity flexibility. Instead, the SDT has expanded the description of vendor in the rationale section. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

As stated in FERC Order 829, section 59, "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". R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59.

If Future is added, the NSRF request that "Future" needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then the NSRF request a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.

The SDT should update R1 to clearly state this, such as;

"R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts concerning the procurement of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: "

This proposed update aligns with FEERC Order 829, section 59 and clearly informs the applicable entity in what is required in future endeavors. R1 will fulfill the FERC directive of having supply chain risk management plans for future procurement, which falls in line with the SDT's "Notional BES Cyber System Life cycle" model. The NSRF does not agree with the "if applicable" wording and the addition of :" associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets", as this is not within the FERC Order.

R1.1 and its parts seem to be disjointed. The NSRF understands to have a Plan (R1) to mitigate cyber security risks to the future procurement of BES Cyber Systems, etc. Within the Plan, entities are to use controls in **their** BES Cyber System planning and development "phase" (which is taken as the Entity's internal processes of wants and needs). To have controls during the "planning and development" phase will not have an impact on the procurement of a BES Cyber System, etc., since nothing is occurring; this is a planning phase, only. Entities are only discussing their wants and needs. This is similar to the caveat within the NERC Defined term of Operating Instruction; (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.) R1.1 has two parts that should address what is required to occur within the plan concerning the objective of R1.1.

Recommend R1.1 to read "The use of controls for BES Cyber Systems to:"

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services; and" (unchanged for the proposed draft). This updated wording of R1.1, directs the use of controls within the plan of R1 and R1.1 states use controls to accomplish the attributes of R1.1.1.

Then R1.1.2, states the Entity is to "…**evaluate methods to address** identified risk(s)". As written, the Entity is to review (address?) their **methods** to mitigate identified risk(s). Without saying, does this part need to be within the proposed Standard? The intent is to mitigate any known risks, not evaluate **methods** to identify risk(s). This could be viewed as an entity's **method** of industry trends to see what new "processes" there are to "evaluate methods to address identified risk(s). Or is this required in order to keep the "how and what" an entity does up to date and current with known "identify and assess" practices. If so, please clarify.

It may be less ambiguous if R1.1.2 is rewritten to read; "Evaluate mitigation methods to address identified risk(s)". This clearly supports R1 where the Requirement states "…controls for mitigating cyber security risks…".

Request that R1.2.parts be updated so Entities will clearly know their expectations under this proposed Standard:

R1.2.1, Process(es) for receiving notification of vendor identified security events; or "Process(es) for receiving notification and release notes of vendor identified security events;

Justification: this updated wording will establish agreed upon processes between the vendor and entity.

R1.2.2, Process(es) for being notified cation when vendor employee remote or onsite access should no longer be granted;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and that the entity need to be kept current on who is authorized by the vendor and allowed by the entity to access BES Cyber Systems.

1.2.3, Process(es) for disclosure of known applicable system vulnerabilities;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and not present a catch 22 when a vendor does not share applicable system vulnerabilities. We also request the "applicable system" be added (as above). Entities may have other vulnerabilities that will not impact the entity's applicable system.

1.2.4, Coordination of response to vendor-related cyber security incidents;

No change.

1.2.5. Process(es) for verifying software integrity and authenticity of all applicable software and patches that are intended for use;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and relates R1.2.3 since the vendor disclosed a vulnerability. Suggest rewording to ensure that it only applies to situations where the vendor provides means to verify software, since standard does not impose requirements on vendors, Responsible Entity would otherwise be forced into non-compliance.

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

No change.

1.2.7. Other pProcess(es) to address risk(s) as determined in Part 1.1.2, if applicable.

Justification: The use of the word "other" is too broad based and could be viewed as all processes, even those outside of the NERC arena. With the clause of "... in Part 1.1.2, if applicable" clearly points to the identified risks of R1.1.2.

Within R1, R1.2, the SDT added the clause, "if applicable" as it relates to EACMS, PACS and PCA's and the NSRF has concerns with this. As written in the proposed Standard's rational box, this item is covered in P.59. FERC Order 829, P. 59, in part states:

"59. 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".

FERC does not state the use of EACMS, PACS and PCA's, but rather "…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" (emphasis added).

By the SDT interpreting P 59 to mean EACMS, PACS and PCA's, this unnecessarily expands the scope of this proposed Standard above and beyond the FERC directive. The NSRF views this as, 1) future contracts concerning security concepts and 2) that support BES operations, which is the BES Cyber Systems identified per CIP-002-5.1a, only. Notwithstanding that EACMAS and PACS is not associated with Low impact BES Cyber Systems. Recommend that R1 and R1.2 have the "if applicable, EACMS, PACS and PCA's" clause deleted. This will allow the

Responsible Entity to have their own risk based controls within their supply chain risk management plan(s) based on the definition of BES Cyber System.

Additional NSRF concerns:

The following statement is taken directly from the Rationale for Requirement R1: "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This, in our opinion, is not conveyed in the written standard's requirement. Though vendors are not intended to be affected by this standard's requirements, Registered Entities will be forced to shy away from purchasing software from companies that cannot meet this standard. We see Regional Entities' Enforcement teams having a difficult time in upholding any possible violations with this standard.

R1. Comments

When it states "if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" what is their intent with the word applicable? It should either be applied or not applied to the systems. If the intent is to give the decision to the Registered Entities make this clearer, or remove the non-BCSs, completely.

R1.1.2 Comments

Add "mitigation" to methods. The intent is to alleviate an identified assessed risk.

Likes 2	Platte River Power Authority, 5, Archie Tyson; OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	

The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
• Recommend rewording Requirement 1 to: "Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets, ***to specifically address the risk of introduction of malicious code through the supply-chain process.*** The plan(s) shall address:" This addition clearly scopes the plan without relying on the title alone to hint at the proper scope. • Is 1.1.2 only evaluating or is it evaluating and implementing?	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	

The expressions, “Identify and assess risk(s),” in R1.1.1 and, “Evaluate methods to address identified risk(s),” in R1.1.2 are unsuitably vague. TFE opportunity is needed, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses). Terms such as, “vendor security event,” should be defined or removed. R1.2.2 conflicts with CIP-004-6 R5 and should therefore be deleted. R1.2.5 is largely duplicative of R3 and R5 of the standard. They should be made consistent, or one of them should be deleted. R1.2.6 is largely duplicative of R4 of the standard. They should be made consistent, or one of them should be deleted. The R1 Rationale statement that CIP-013-1, “does not require the Responsible Entity to renegotiate or abrogate existing contracts,” implies that no action needs to be taken for existing PEDs. This point should be made explicit in the standard per se, but our “additional comments” concerns would still apply for replacing or upgrading existing equipment.	
Likes 0	
Dislikes 0	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	

Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
R1 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R1 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R1 should be rewritten to be only applicable to high and medium impact BES Cyber Systems	
Likes 0	
Dislikes 0	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	
Requirement 1 should state specifically, as to its purpose, to prevent the introduction of malware or malicious code through the supply-chain process. There should be an official NERC definition of the term 'Vendor(s)'. Although the Rational and Guidelines for each define the term, there should be a more official definition in order to provide appropriate guidance for the auditors when evaluating compliance to this standard.	

What does Requirement 1.1.2 mean? ... The plan(s) shall address: The use of controls … to: Evaluate methods to address identified risk(s). If a risk is identified during procurement and deployment, are we only required to evaluate methods to address those risks – or *address* the risks? This is incredibly confusing and leaves this requirement wide-open to interpretation. The rational for Requirement R5 is identified as being based on FERC Order 829 (page 48), which specifically addresses Vendor Remote Access to BES Cyber Systems, without respect to applicability – Sections 76-80. Multiple requirements are referenced in Standards CIP-004, CIP-005 and CIP-007 that are only applicable to High and/or Medium Impact BESCS with weaknesses identified by not directly addressing vendor initiated machine-to-machine remote access. In the final sentence of Section 80, it is noted that vendor remote access is not adequately addressed in the 'Approved' standards and, therefore, is an objective that must be addressed in the supply chain management plans. Again, there is no reference to applicability, whereas the meat of the directive covers approved standards that reference Medium and High impact BESCS. The scope and content of the already approved standards is the appropriate place to account for this weakness. A full impact and applicability analysis should be performed prior to proposed modification(s).	
Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Change/add language to emphasize that failure to obtain the cyber security controls from a vendor doesn't translate to being out of compliance. Entity should have the ability to mitigate risks posed by vendors. IID feels that the SDT should consider modifications to current CIP standards where the topic is already addressed.	
Likes 0	

Dislikes 0	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	

1. The standard lacks clarity on addressing R1.2 sub-requirements where no relationship of any sort exists between a RE and vendors whose products may be installed on applicable systems.

Many software and hardware components utilized on BES Cyber Systems, associated EACMS, PCA, and PACS systems are provided without any contractual agreement other than acceptance of a End-User-License-Agreement (EULA) upon installation.

For example, the Java Resource Environment, which is provided by Oracle Corporation, is utilized by many products. However, there is no agreement or financial transaction associated with the acquisition of Java.

This is even further complicated where open-source software is utilized for which no formal organization holds responsibility.

Finally, some proprietary software is acquired without any contractual arrangements due to low acquisition costs, such as an SSH client for less than $200.

In the case where there is a lack of relationship and/or financial interest in establishment of a formal agreement, how can RE address the provided requirements?

2. What incentive does a vendor have to disclose their vulnerabilities to a client? Wouldn't this disclosure ultimately serve to publicize the vulnerabilities?

Responsible entities can request this cooperation, but verification that the vendor is disclosing all vulnerabilities is not possible.

Likes 0	

Dislikes 0	
Eric Ruskamp - Lincoln Electric System – 6	
Answer	No
Document Name	
Comment	

During the CIP-013-1 webinar on Feb 2, the SDT indicated several times that it is not the intention of R1 to force vendors to perform actions so that entities can comply with the standard. R1.2.1, R1.2.2, R1.2.3 would force vendors to develop internal processes to notify entities of any changes relating to the requirements which would force vendors to take independent action to notify entities of any changes. Also, during the procurement phase, why would vendors reveal potential security flaws in their product above and beyond normal security patch notifications while they are competing against other vendors for the entities business? This seems like wishful thinking. Also, entities have processes in place already for other CIP requirements to fully prepare an asset for deployment into the ESP. We don't grab equipment off of the back of the delivery truck and deploy it into the ESP immediately so what is the point of knowing about security flaws in their products during procurement? Any security flaws are probably already addressed with patches that will be downloaded and installed when preparing the asset for deployment. Also, a vulnerability assessment has to be performed against the asset and CIP-007/CIP-005 security controls have to be checked prior to deployment. 1.2.1, 1.2.3, 1.2.4 appear to be redundant with CIP-007 R2 security patch management. Is the SDT expecting vendors to provide information about security/design flaws above and beyond the normal security patch notifications? If so, what kind of information would that be?

1.2.5 is troublesome as well (and it seems to be a duplicate of R3). Entities typically use update or proxy servers to discover and identify applicable security patches. For example, we use Windows Update Server Services to identify patches and roll them out once testing and approvals are complete. Do we need to check the check sums of the identified patches or can we trust that the update servers are authenticating the software?

Likes 0	
Dislikes 0	

Deborah VanDeventer - Edison International - Southern California Edison Company - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SCE agrees with this requirement in concept. However, as written, this requirement contains several issues that SCE believes should be resolved. The language of CIP-013-1 Requirement R1 does not clearly state what is required and is open to several interpretations. For example, Requirement R1, 1.1 requires the use of controls to identify and assess risks during the procurement and deployment of vendor products and services. However, consistent with the COSO framework, a risk methodology identifies and assesses risks, and controls are used to mitigate those identified risks. In addition, the requirement and its subparts do not define the security objective. This lack of clarity in the language of Requirement R1 may pose issues during audit. We recommend the following language to clarify the requirement consistent with intent of the FERC Order No. 829 directives:

R1. Each Responsible Entity shall define, document, and implement one or more supply chain risk management methodologies(s) that address objectives, risks, and controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The defined methodologies(s) shall define controls used to mitigate the risks of entering into contracts with vendors who pose significant risks to responsible entity's information systems, of procuring products that fail to meet minimum security criteria, and of failing to receive adequate notice from compromised vendors, and shall include: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

1.1 The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:

1.1.1 Process(es) for notification of vendor security events;

1.1.2 Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.1.3 Process(es) for disclosure of known vulnerabilities;

1.1.4 Coordination of response to vendor-related cyber security incidents; 1.1.5 Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use; 1.1.6 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and 1.1.7 Other process(es) to address risk(s) as determined, if applicable.	
Likes 0	
Dislikes 0	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests further clarification from the drafting team on R1 and whether it applies to Low impact BES Cyber Assets. Since the current language of the requirement is silent on the level of applicability, an entity may assume that R1 applies to all High, Medium, and Low Impact BES Cyber Systems. Duke Energy disagrees with the concept of applying R1 to Low Impact BES Cyber Systems. At the outset, Low Impact BES Cyber Systems have been subject to a risk assessment and classified as Low Impact since they pose a minimal threat to the BES. Also, a Responsible Entity is not obligated to have an inventory list of its Low Impact BES Cyber Systems. In the rationale section of R5, it is even mentioned that a list of Low Impact BES Cyber Assets is not required. Without a list of Low Impact BES Cyber Systems, we fail to see how a Responsible Entity could demonstrate compliance with R1. For this reason, coupled with the fact that the Low Impact BES Cyber Systems pose a minimal risk to the BES, we do not believe R1 should be applicable to Low Impact BES Cyber Systems, and the requirement language should reflect the applicability.	

Duke Energy requests confirmation that the rationale provided in R1 (and throughout the standard) be included in the standard, even after the standard has been finalized and approved. We feel that some of the language in the rationale is very useful, and that some of the language is warranted in the requirement(s) themselves. Specifically, the phrase used in the rationale of R1:

"Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

We feel that this language is significant enough as it pertains to R1.2 and the possibility of disagreement between an Entity and an external party, that it should be placed somewhere in the standard.

Lastly, we recommend the drafting team consider developing this standard similarly to CIP-002-5.1a with regards to the leveraging of a bright-line model of risk assessment. This will ensure that entities are assessing risk consistently of their vendors and removes the potential disagreement in audit that a regulator finds that the entity's risk determination is incorrect based on a different set of subjective criteria. This was the justification needed to move from the risk-based assessment methodology (RBAM) in CIP Versions 1 – 3 to the bright-line criteria developed in CIP Version 5.

Likes 0	
Dislikes 0	

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	

We have four concerns with the proposed requirement.

First, CIP-013 should follow the other CIP Standards with respect to Low BES Cyber Assets. R1 should clearly exclude Low BES Cyber Assets and refer to R5 for those assets, and all requirements related to Low BES Cyber Systems should be consolidated into R5.

Second, we are concerned that the difference in wording between R 1.1 which refers only to BES Cyber Systems, and R1.2 which includes EACMS, PACS and PCAs, is confusing and can cause inconsistencies in implementation. R1.1, and subsequently R1.2, should be rewritten to help with this. Please consider the following suggestions:

From: *"1.1 The use of controls in BES Cyber System planning and development to:"*

To: *"1.1 The use of controls in planning and development to:"*

From: "*1.2 The use of controls in procuring vendor product(s) or service(s) that address the Following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:"*

To: *"1.2 The use of controls in procuring vendor product(s) or service(s): "*

Third, we believe that the term "cyber security incident" in R1.2.4 should be capitalized to be clear that it is to be interpreted as the NERC-defined term "Cyber Security Incident".

Fourth, for consistency and clarity, we request the term 'supply chain risk management' be 'supply chain cyber security risk management' throughout the standard and guidance.

Likes 2	PPL - Louisville Gas and Electric Co., 6, Oelker Linn; Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
ALAN ADAMSON - New York State Reliability Council – 10	
Answer	No
Document Name	
Comment	

See NPCC comments.	
Likes 0	
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company – 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Mark Riley - Associated Electric Cooperative, Inc. – 1	
Answer	No
Document Name	
Comment	
AECI contends that R1 should be separated into two distinct requirements. R1 should be revised to require the Responsible Entity to develop and document supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems... The SDT should then develop an additional requirement (R2) to require the Responsible Entity to implement the documented supply chain risk management plan(s) documented in R1.	

In addition to the comments above, AECI supports the following comments submitted by the MRO NRSF:

"As stated in FERC Order 829, section 59, "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". R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59.

If Future is added, the NSRF request that "Future" needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then the NSRF request a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant."

Furthermore, AECI urges the SDT to use the supply chain definition from NIST Special Publication 800-53 Rev.4 that was identified in paragraph 32, footnote 61 in this requirement.

Likes 0	
Dislikes 0	
Mick Neshem - Public Utility District No. 1 of Chelan County – 3	
Answer	No
Document Name	
Comment	

CHPD has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate

the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives. CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5. CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.” CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions). CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used. For R1.1.2 CHPD requests changing the word *evaluate* to *determine.* For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used. For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”	
Likes 0	

Dislikes 0	
Tyson Archie - Platte River Power Authority – 5	
Answer	No
Document Name	
Comment	

Platte River Power Authority (PRPA) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

PRPA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, PRPA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, PRPA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required, low with a reduced set of requirements to address their lower risk, PRPA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

PRPA requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

PRPA is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see PRPA’s response to Question #9 for additional information on exceptions).

PRPA notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 PRPA requests changing the word *evaluate* to *determine.* For R1.2.1 PRPA requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used. For R1.2.1 PRPA requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. PRPA requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Steven Mavis - Edison International - Southern California Edison Company – 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Andrew Gallo - Austin Energy – 6	
Answer	No
Document Name	

Comment
Austin Energy (AE) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives. AE does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, XXX requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, XXX believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, XXX requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5. AE requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.” AE is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see XXX’s response to Question #9 for additional information on exceptions). AE notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used. For R1.1.2 AE requests changing the word *evaluate* to *determine.* For R1.2.1 AE requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used. For R1.2.1 AE requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. AE requests additional language in the requirement that addresses

"entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."	
Likes 2	Austin Energy, 4, Garvey Tina; Austin Energy, 3, Preston W. Dwayne
Dislikes 0	
Brian Evans-Mongeon - Utility Services, Inc. – 4	
Answer	No
Document Name	
Comment	

1. The Rational for Requirement R1 includes a definition of the term "vendors". This definition is also included in the Guidelines and Examples document. This term should be officially defined in the standard or added to the NERC Glossary of Terms and capitalized when used.

2. It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3. R1.1 is vague in the language used with terms like "assess risk" and "evaluate". The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:"The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team's professional judgement cannot override the determination made by the Responsible Entity. "

4. For R1: This requirement requires both the development and the implementation of a plan. We recommend modifying this requirement into three steps which follows the CIP-014 structure – Entity to 1) identify risk, 2) develop a plan, 3) develop an

implementation timeline. The timeline should use fixed dates or intervals and not dates that are linked to the completion of other compliance activities

5. For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This should be incorporated into the Requirement itself.

6. For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list "planning, acquisition and deployment" and versions of these terms in the diagram. R1.1 uses "planning and development". The meaning of "development" has not been clarified and is not part of the process addressed by this standard. Suggest that "development" be clarified or removed.

7. The standard as written addresses Vendor Risk Management and no other supply chain risks such as sole source and international dependencies. Suggest changing the name, purpose, and other areas of the standard from supply chain" to "vendor".

8. For R1.1.2:

   i. We recommend changing *evaluate* to *Determine.* We also seek further clarification of the intent. As, written the requirement is ambiguous:

      a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

      b. to evaluate the effectiveness of mitigating that risk? or;

      c. is it meant to identify what controls you have to mitigate the risks you have?

   ii. The evaluation of methods is a administrative task and similar to other tasks removed from the NERC standards as part of the Paragraph 81 project.

9. For R1.2.1: The words "Security Event" are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then this should be an officially defined term either in the standard or in the NERC glossary. The s definition provided in the glossary is "any identified, threatened, attempted or successful breach of vendor's components, software or systems" and "that have potential adverse impacts

to the availability or reliability of BES Cyber Systems" It is unclear if the second portion is meant to be part of the definition. Many cyber systems, like firewalls, are under constant threat and attempts to breach the systems security. Suggest replacing "vendor security event" with "identification of a new security vulnerability". Vendors may not be able to determine if a vulnerability "could have potential adverse impact to the availability or reliability of BES Cyber System". This clause would only be applicable in determining when an entity would notify a vendor.

10. For R1.2.1: Page 6, line 12 of the Guidance and Examples document list both notification of security events from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both types of notifications.

11. For R1.2.1: The requirement for the" process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document.

12. For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document The requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that "A failure of a vendor to follow a defined process is not a violation of this Requirement."

13. Page 6, line 12 of the guidance details the notification of the vendor by the entity. It is unclear that the R1.2.1 requires notification by the entity to the vendor as detail in the guidance document.

14. Recommend that "Security Event" be changed to require the reporting of only newly identified security vulnerabilities.

15. Change 1.2.7 from pointing to 1.1.2 to 1.1.1. Remove 1.2 since 1.2.7 covers 1.2.

16. Do not agree with the current draft language that includes all High, Medium and Low BES Cyber Systems in Requirement R1. Suggests limiting this requirement to High and Medium only as the current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. If controls are needed for low impact, suggest moving these to R5 to consolidate all low impact into a single requirement.

17. The SDT needs to make sure that there is no duplication in the standards. Provide guidance on how areas that seem to overlap like Interactive Remote Access and CIP-005.

18. Request the SDT to consider adding the following language from the rationale to the language of the standard "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

19. The Rationale for R1, it states that R1, P1.1 addresses P 56 of Order No. 829. P 56 calls for a risk assessment of the entities internal systems with this language "how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes". R1, P1.1.1 calls for a risk assessment of the vendors systems with this language "procurement and deployment of vendor products and services." The language in the order does not match the language in the standard and therefore suggest that the language be consistent to provide clarity.

20. There could be an impact of contract requirements on the ability of public utilities to piggyback on wide-area contracts such as those of National Association of State Procurement Officials (NASPO) Cooperative, Western States Contracting Alliance (WSCA), Washington State Department of Enterprise Service, and others. Recommend that a exclusion be permitted in the case of such contracts, which are important to provide flexibility and negotiating strength for public utilities throughout the country. Include language that provides an exclusion for contracts that are covered by other laws or regulations.

21. The requirement should not reference the word "mitigation". Suggest that "mitigate" be replace with "address" as listed in R1.2.

22. Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

Likes 0	
Dislikes 0	

Janis Weddle - Public Utility District No. 1 of Chelan County – 6

Answer	No
Document Name	
Comment	

Public Utility District No. 1 of Chelan County (CHPD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."	
Likes 0	
Dislikes 0	
Haley Sousa - Public Utility District No. 1 of Chelan County – 5	
Answer	No
Document Name	
Comment	

The Public Utility District No. 1 of Chelan County (CHPD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD’s response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

Likes 0	
Dislikes 0	
W. Dwayne Preston - Austin Energy – 3	
Answer	No
Document Name	
Comment	

I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 – FRCC	
Answer	No
Document Name	
Comment	
R1.1 The lack of guidelines and technical basis within a balloted and approved standard itself (not in a separate document) will result in many different interpretations and expectations on how to meet the requirement. As demonstrated in the measures section, the section lacks specificity as potentially every correspondence with a vendor is subject to data request and audit. Who is the vendor? Is it the manufacturer/software company, the reseller the hardware/software is acquired from, the shipping company, the integrator, others? For temporary staff, is the contract employee a vendor? These are just example questions. A lack of guidelines and technical basis within the standard itself could result in a broad interpretation of R1.1 that provides higher risk with little or no additional security. As entities will have to guess the auditor's interpretation, it increases the likelihood that a standard will be violated due to poor definition. R1.2 This requirement should define a specific minimum security standard in a manner that avoids the inefficiencies from hundreds of entities performing the same analysis. This inefficiency adds costs to entities and to vendors for items that will be passed on to entities. As written, only concepts are presented, not a minimum specification that entities and vendors can effectively use to cost effectively demonstrate compliance in a consistent manner across the industry.	
Likes 0	
Dislikes 0	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Chad Bowman - Public Utility District No. 1 of Chelan County – 1	
Answer	No
Document Name	
Comment	
CHPD has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives. CHPD does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CHPD requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CHPD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower	

risk, CHPD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

CHPD requests that the SDT add the following language from the rationale to the language of the standard: "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

CHPD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see CHPD's response to Question #9 for additional information on exceptions).

CHPD notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CHPD requests changing the word *evaluate* to *determine.*

For R1.2.1 CHPD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CHPD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. CHPD requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

Likes 0	
Dislikes 0	
Lona Hulfachor - Salt River Project - 1,3,5,6 – WECC	
Answer	No
Document Name	

Comment

SRP has an active role on the CIP-013 SDT with an employee serving as a member of the team as well as our support staff who are participating in the SDT meetings. In addition, SRP has been engaging in dialogue with peers of trade associations such as LPPC to address the CIP-013 standard development activities.

SRP continues to be a strong supporter of efforts that ensure the security of the Bulk Electric System. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order, while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

SRP does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, SRP requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, SRP believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required for low impact assets, with a reduced set of requirements to address their lower risk, SRP requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

SRP requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

SRP is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see SRP’s response to Question #9 for additional information on exceptions).

SRP notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 SRP requests changing the word *evaluate* to *determine.*

For R1.2.1 SRP requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 SRP requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. SRP requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Steven Rueckert - Western Electricity Coordinating Council – 10	
Answer	No
Document Name	
Comment	
No objections to R1.1. Although the actual language of R1.2 seems sound, how does this language in the R1 rationale section , "***For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan***" (Section B, p. 5) manage risks associated with Supply Chain Management vendors? Where is the incentive for an entity to actively pursue vendor negotiations to minimize risks during the procurement phase? Merely adding control elements to an RFP that are not subsequently incorporated through vendor negotiations into a product or Service Level Agreement [SLA] seems to be nothing more than an academic exercise. At a minimum, under the current rationale the entity should provide working documents (as described in M1) of the negotiations process to demonstrate compliance with R1.2?	
Likes 0	
Dislikes 0	
John Hagen - Pacific Gas and Electric Company – 3	

Answer	No
Document Name	
Comment	

The following language from the rational box for Requirement R1 does not seem to incentivize an entity to actively pursue vendor negotiations to minimize risks during the procurement phase.

For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Merely adding control elements to an RFP that are not incorporated through vendor negotiations seems to be nothing more than an academic exercise. At a minimum, under the current rational, the entity should provide working documents of the negotiations process to demonstrate compliance with R1.2. Extending the initial review and update, as necessary

Likes 0	
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation – 4	
Answer	No
Document Name	
Comment	

- The extent of the "supply chain risk management plan" should be more clearly defined. The Requirement language goes beyond what is typically considered "supply chain" activities (i.e. activities involving the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer) and includes ongoing operational protections. The Standard should more clearly define what is meant by "supply chain" and limit the associated Requirement to mitigating the associated risks. All other

operational related protections should be addressed within the existing CIP Standard that already cover the related protections (e.g. remote access controls should be included in CIP-007 and not in a supply chain standard).

- The R1 Supply Chain Risk Management plan is applicable to BES Cyber Systems of all impact levels (and any associated EACMS, PACs, and PCAs). The following recommendations are provided:

o The inclusion of Low Impact BES Cyber Systems in the scope of the Supply Chain Risk Management Plan should be reconsidered. The existing CIP-002-5.1 and CIP-003-6 only requires an entity to identify asset(s) containing Low Impact BCS and does not require a documented inventory of low impact BCS/BCA or even a documented list of system/asset types. The expectations of the Requirement would make it very difficult for an Entity to demonstrate compliance without a list of Low Impact BCS/BCA.

o If after reconsideration it is still deemed necessary to include Low Impact BCS within the scope of the Supply Chain Risk Management Plan, the supply chain Requirement should be removed from CIP-013 and added to CIP-003 with the rest of the requirements that are applicable to Low Impact BCS. SDTs have made conscious decisions to keep all Requirements applicable to Low Impact BCS within the CIP-003 Standard and not have them sprinkled throughout all the CIP Standards. Additional time should be taken in developing the standard to remain consistent with this approach. (Note: Reference the CIP-003-7i draft CIP Standard related to low impact BES System Transient Cyber Assets.)

- For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months.

- Use of the “Notional BES Cyber System Life Cycle” model is problematic. Entities plan and assess future cyber systems, but acquire, configure, deploy, and maintain individual cyber assets.

- R1 – 1.2.1, 1.2.3, 1.2.4 references to vendor security events, vulnerabilities, and incidents are undefined and potentially overly broad. Auditors may not collectively or individually agree with an individual RE’s assessment of how these terms are defined and used within their R1 Plan.

- R1 – appears to overlap with parts of several existing CIP Standards, including: CIP-003-6 R2 Att. 1, Section 3; CIP-004-6 R4.1 - 4.4 and R5.1 - 5.5; CIP-005-5 R2.1 - 2.3; CIP-007-6 R2.1, R5.1, 5.5, 5.6, 5.7; and CIP-010-2 R1.1. Expanding the scope of these existing CIP programs

with a new Standard could unintentionally disrupt or conflict with current security architectures and/or critical operations. FE recommends that the SDT consider making coordinated modifications to the scope and applicability of CIP-003, 004, 005, 007 and 010, at some future date, rather than extending existing requirements to a new Standard, i.e. CIP-013. FE suggests that the scope of the Supply Chain Standard include the administrative controls needed to address Order 829, and the operational and technical security controls remain in the existing CIP standards. • Measures and Evidence – Since the R1 requires an entity to show that the plan has been implemented, M1 does not adequately describe the evidence required to demonstrate implementation of the plan, i.e. especially for technical sub-requirements. (For example the evidence that an entity has implemented, "1.2.1 Process(es) for notification of vendor security events," would likely require a process map for how vendor notifications are received, processed and resolved. Additionally, an auditor would likely want a sample of actual dated notifications from several vendors with dated evidence of consistent action and resolution.) FE recommends that the SDT provide additional guidance on evidence types, formats etc… similar to what was provided in CIP-003-6 Attachment 2.	
Likes 0	
Dislikes 0	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 – NPCC	
Answer	No
Document Name	
Comment	
Please refer to RSC- NPCC comments	
Likes 0	
Dislikes 0	
Aubrey Short - FirstEnergy - FirstEnergy Corporation – 1	

Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative – 5	
Answer	No
Document Name	
Comment	

R1, R2, and R5 contain obligations that apply to low impact BES Cyber Systems. With the inherent low risk that comes with these systems, Basin Electric questions whether the same protections for highs and mediums should be applicable to lows, especially in context of R1. Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013. Basin Electric is concerned the inclusion of lows will necessitate maintaining a list of low BES Cyber Systems and possibly a list of low BES Cyber Assets.

As stated in FERC Order 829, section 59, "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". R1 does not align with the above FERC directive. FERC clearly insisted that future contracts will address the five attributes of section 59.

If Future is added, Basin Electric requests that "Future" needs to be better defined. If a company has a contract that is multi-year and each year a new Purchase Order is issued, the contract is not new or revised. There needs to be direction given on how to implement the requirements of the standard going forward.

If Future is not added, then Basin Electric requests a possible foot note stating… that R1 applies to all contracts (agreements) starting on the date of enforcement of CIP-013-1. As FERC has stated in FERC Order 693, section 253, Entities need to satisfy the Requirements in order to be compliant.

The SDT should update R1 to clearly state this, such as:

"R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts concerning the procurement of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. The plan(s) shall address: "

This proposed update aligns with FERC Order 829, section 59 and clearly informs the applicable entity in what is required in future endeavors. R1 will fulfill the FERC directive of having supply chain risk management plans for future procurement, which falls in line with the SDT's "Notional BES Cyber System Life cycle" model. Basin Electric does not agree with the "if applicable" wording and the addition of :" associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets", as this is not within the FERC Order.

R1.1 and its parts seem to be disjointed. Basin Electric understands to have a Plan (R1) to mitigate cyber security risks to the future procurement of BES Cyber Systems, etc. Within the Plan, entities are to use controls in **their** BES Cyber System planning and development "phase" (which is taken as the Entity's internal processes of wants and needs). To have controls during the "planning and development" phase will not have an impact on the procurement of a BES Cyber System, etc., since nothing is occurring; this is a planning phase, only. Entities are only discussing their wants and needs. This is similar to the caveat within the NERC Defined term of Operating Instruction; (A discussion of general information and of potential options or alternatives to resolve Bulk Electric System operating concerns is not a command and is not considered an Operating Instruction.) R1.1 has two parts that should address what is required to occur within the plan concerning the objective of R1.1.

Recommend R1.1 to read "The use of controls for BES Cyber Systems to:"

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services; and" (unchanged for the proposed draft). This updated wording of R1.1, directs the use of controls within the plan of R1 and R1.1 states use controls to accomplish the attributes of R1.1.1.

Then R1.1.2, states the Entity is to "…**evaluate methods to address** identified risk(s)". As written, the Entity is to review (address?) their **methods** to mitigate identified risk(s). Without saying, does this part need to be within the proposed Standard? The intent is to mitigate any known risks, not evaluate **methods** to identify risk(s). This could be viewed as an entity's **method** of industry trends to see what new "processes" there are to "evaluate methods to address identified risk(s). Or is this required in order to keep the "how and what" an entity does up to date and current with known "identify and assess" practices. If so, please clarify.

It may be less ambiguous if R1.1.2 is rewritten to read; "Evaluate mitigation methods to address identified risk(s)". This clearly supports R1 where the Requirement states "…controls for mitigating cyber security risks…".

Request that R1.2.parts be updated so Entities will clearly know their expectations under this proposed Standard:

Please add clarification to what is meant by vendor "services" as stated in R1.2.

R1.2.1, Process(es) for receiving notification of vendor identified security events; or "Process(es) for receiving notification and release notes of vendor identified security events;

Justification: this updated wording will establish agreed upon processes between the vendor and entity.

R1.2.2, Process(es) for being notified when vendor employee remote or onsite access should no longer be granted;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and that the entity need to be kept current on who is authorized by the vendor and allowed by the entity to access BES Cyber Systems.

1.2.3, Process(es) for disclosure of known applicable system vulnerabilities;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and not present a catch 22 when a vendor does not share applicable system vulnerabilities. We also request the "applicable system" be added (as above). Entities may have other vulnerabilities that will not impact the entity's applicable system.

1.2.5. Process(es) for verifying software integrity and authenticity of all applicable software and patches that are intended for use;

Justification: this updated wording will establish agreed upon processes between the vendor and entity and relates R1.2.3 since the vendor disclosed a vulnerability. Suggest rewording to ensure that it only applies to situations where the vendor provides means to verify software, since standard does not impose requirements on vendors, Responsible Entity would otherwise be forced into non-compliance.

1.2.7. Process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

Justification: The use of the word "other" is too broad based and could be viewed as all processes, even those outside of the NERC arena. With the clause of "... in Part 1.1.2, if applicable" clearly points to the identified risks of R1.1.2.

Within R1, R1.2, the SDT added the clause, "if applicable" as it relates to EACMS, PACS and PCA's and Basin Electric has concerns with this. As written in the proposed Standard's rational box, this item is covered in P.59. FERC Order 829, P. 59, in part states:

"59. 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".

FERC does not state the use of EACMS, PACS and PCA's, but rather "…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" (emphasis added).

By the SDT interpreting P 59 to mean EACMS, PACS and PCA's, this unnecessarily expands the scope of this proposed Standard above and beyond the FERC directive. Basin Electric views this as, 1) future contracts concerning security concepts and 2) that support BES operations, which is the BES Cyber Systems identified per CIP-002-5.1a, only. Notwithstanding that EACMAS and PACS is not associated with Low impact BES Cyber Systems. Recommend that R1 and R1.2 have the "if applicable, EACMS, PACS and PCA's" clause deleted. This will allow the Responsible Entity to have their own risk based controls within their supply chain risk management plan(s) based on the definition of BES Cyber System.

The following statement is taken directly from the Rationale for Requirement R1: "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This is not conveyed in the written standard's requirement. Though vendors are not intended to be affected by this standard's requirements, Registered Entities will be forced to shy away from purchasing software from companies that cannot meet this standard. We see Regional Entities' Enforcement teams having a difficult time in upholding any possible violations with this standard.

Likes 0	
Dislikes 0	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	
Comment	

For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

1.

i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

ii. To evaluate the effectiveness of mitigating that risk? or;

iii. Is it meant to identify the controls in place to mitigate the identified risks?

Revise R1.2.1 as follows, "Process(es) for notification of vendor security events **that affect BES reliability**;"

For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

It is not clear if R1 applies to High, Medium and Low since R3, R4 and R5 specify the impact level. This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

R1.1 is vague in the language used with terms like "assess risk" and "evaluate".

Concern that the Entity interpretation can be very different than Auditor interpretation. Once an entity has completed its risk evaluation, this determination cannot be overturned by the Regional Entity. Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1 The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text: • "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts." • "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
William Harris - Foundation for Resilient Societies - 8	
Answer	No

Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See overview comments and comments specific to Req2uirement R1, in attached file.	
Likes 0	
Dislikes 0	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

Both the draft guidance document and the “Rationale for Requirement R1” section of the draft Standard contain the statement, “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” However, there is nothing in any Requirement or any Requirement Part containing such language. Language similar to existing technical feasibility language in CIP-002 through CIP-011 should be added.

N&ST considers requirement part 1.2.2 redundant with existing CIP-004-6 Requirements R4 and R5 and recommends that either it be deleted from this Standard or modified to indicate a Responsible Entity may address it with existing CIP-004 access management procedures.

N&ST considers requirement part 1.2.6 redundant with existing CIP-005-5 Requirements R1 and R2 and recommends that either it be deleted from this Standard or modified to indicate a Responsible Entity may address it with existing CIP-005 procedures for Electronic Access Points and for Interactive Remote Access.

N&ST also recommends that all "Vendor remote access" requirements relevant to supply chain management be presented in one top-level requirement, not in two (R1 and R4). N&ST also recommends that all "Software integrity and authenticity" requirements be presented in one top-level requirement, not two (R1 and R3).	
Likes 0	
Dislikes 0	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
We recommend the drafting team remove the phrase "if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" from the language of Requirement R1 and Section 1.2 because, we feel that this language is inconsistent with FERC Order 829 Directive language. Also, we suggest that the drafting team add some clarity to the sub-parts of Section 1.2 so that the industry will clearly know their expectations. In reference to Requirement R1 and contracts, we suggest that the term "future contracts" be included in the proposed language of the Requirement. Also, we suggest the drafting team develop a definition for the term "future contracts" that would potentially include the phrase "new or modified contracts on or after the date of Enforcement" in the proposed definition. SPP's proposed language revision to R1: "Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to future contracts pertaining to the procurement of the BES Cyber System."	

Finally, we feel that the Measurement and Requirement language is inconsistent with the sub-part language. In the second sentence of the Requirement and Measurement the term “mitigating” is used, and we suggest replacing the term with “addressing”. We need to ensure all of our risk management options are available to us.	
Likes 0	
Dislikes 0	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	
Comment	

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and

machine-to-machine remote access.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and machine-to-machine remote access.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level? 1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same? 1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance. 1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan? 1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access? Add the forward-looking language to the standard, itself. Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?	
Likes 0	
Dislikes 0	
Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No

Document Name	
Comment	

We commend the drafting team for attempting to meet the directives and respect their effort and commitment to that end. We agree with now acting FERC chair LaFleur's comments in her dissent on Order 829, "The Commission is issuing a general directive in the Final Rule, in the hope that the standards team will do what the Commission clearly could not do: translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act."

We do not agree with the approach in R1 (and R2) of creating "plans" and the intent of the plans to "cover the procurement aspects of all four objectives."

Order 829's four objectives did not include creating "plans." All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011.

Standards will not be effective, auditable or enforceable with a CIP-013 standard dueling with CIP-002 through -011 on scope and obligations.

CIP-002 through -011 are the appropriate place to address these operational security controls. These standards establish the least ambiguity in scope of obligations. These standards make granular distinctions based on risk when assigning what BES Cyber Assets are subject to each requirement. The risk distinctions go beyond just low, medium or high impact and incorporate Control Center, External Routable Connectivity and Interactive Remote Access in assigning obligations for requirements.

NERC's Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets and all have very different risks to the grid and different obligations under CIP-002 through CIP-011.

"Plans" cannot achieve an effective, auditable and enforceable standard for 1,398 NERC entities that address the complicated issues identified in LaFleur's dissent … and certainly not to meet the September 2017 directed deadline.

Industry can at a minimum advance cyber security by revisions to operational security controls in CIP-002 through -011. Other commenters, including EEI, are submitting examples of language as starting points.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and machine-to-machine remote access.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?	
Likes 0	
Dislikes 0	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Dominion supports the work that the drafting team has performed to-date and understands that the current draft of CIP-013-1 is continuing to evolve. Dominion has developed extensive comments to allow the drafting team to focus efforts on areas of particular concern with the current draft. Dominion supports the team's continued efforts to bring stakeholder knowledge and expertise together to develop an objective based reliability standard that realistically addresses reliability gaps in the cyber supply chain process.

- Dominion has a concern that the specific risks identified in P57 of FERC Order No. 829 are not included Requirement R1. The term used in the current draft of CIP-013-1, "cyber security risks", is overly broad and should be constrained by the enumerated risks in the FERC order.

Constraining language for the term 'cyber security risks' could include" risks associated with the of procurement and installation of unsecure equipment or software, the risks associated with unintentionally failing to anticipate security issues that may arise due to network architecture or during technology and vendor transitions, and the risks associated with purchasing software that is counterfeit or that has been modified by an unauthorized party."

Dominion recommends the development team consider the following language change for R1:

"Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that include security considerations related to cyber security risks related to procuring and installing unsecure equipment or software, the risk of unintentionally

failing to anticipate security issues that may arise due to network architecture, unintentionally arise during technology and vendor transitions, and purchasing software that is counterfeit or that has been modified by an unauthorized party for BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets."

- In addition, Dominion recommends that system applicability should be clearly identified in the Rationale section of the requirement. Specifically, it is recommended that the "to the extent applicable" language should be removed from part 1. 2 and from the Rationale for R1.

- Dominion recommends the following for Parts 1.1.1 and 1.1.2:

i. Identify and assess cyber security risk(s) to the BES, if any, during the procurement and deployment of vendor products and services; and

ii. Evaluate methods to address identified risk(s).

- The term "services" in Part 1.2 is very broad and could be interpreted differently by different parties. To ensure consistent understanding of this term, Dominion recommends that the development team place context around the term 'service' as used in requirement R1.2 in a compliance guidance document.

- Dominion recommends that Part 1.2.7 be removed from CIP-013-1. The comprehensive list of risks in Parts 1.2.1 through 1.2.6 appropriately addresses the risk.

- As an alternative to the above recommendations, the development team could consider the following new proposed requirements in lieu of requirement R1 and R2:

R1: Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that include security considerations related to cyber security risks of 1) procuring and installing un-secure equipment or 2) procuring and installing un-secure software, including purchasing counterfeit software, or software that has been modified by an un-authorized party 3) unintentionally failing to anticipate security issues that may arise due to network architecture, 4) unintentionally failing to anticipate security issues that may arise during technology and vendor transitions for BES Cyber Systems and associated Electronic Access Control or Monitoring Systems, Physical

Access Control Systems, and Protected Cyber Assets. The supply chain plan(s) shall address: 1. 1. Process(es) for notification of vendor security events; 1.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted; 1.3. Process(es) for disclosure by the vendor of known vulnerabilities; 1.4. Coordination of response to vendor-related cyber security incidents; 1.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use; and, 1.6. Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); R2: The supply chain plan(s) shall include a process whereby any risk identified by the vendor during the purchasing process is assessed, reviewed, mitigating activities evaluated, and actions based on the selected mitigating activities implemented prior to placing the item(s) in service. R3: The supply chain plan(s) shall be reviewed, updated as necessary, and approved by CIP SM or delegate at least once every fifteen (15) months. The Rationale should explain that risks 1 and2 are addressed by R1.3 and R1.5, risk 3 by R1.1-R1.4 and R1.6, and risk 4 by R1.2, 1.3, and R1.6. And that the planning and system lifecycle processes are addressed in the order are expected to encapsulate the purchasing process and are covered by R2. 2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.
Likes 0

Dislikes 0	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

In addition to high and medium impact BES Cyber Systems, the applicability of R1 should be clear to include low impact BES Cyber Systems.

SCE&G agrees with the concerns and question raised by the Security Practices Working Group of North American Generator Forum (NAGF) regarding "if applicable":

"The phrase "if applicable" is ambiguous in the language of the main requirement. One reading is that "if applicable" means that the requirement only applies should the device types of associated EACMS, PACS or PCAs actually exist. Another reading is that "if applicable" is based on the risk that an entity places on a particular vendor as part of its documented risk management plan(s). If an entity performs a risk assessment of its vendors and finds that a vendor is a low or potentially zero risk (coupling a vendor's reputation with their particular usage within an entity), does this mean that an entity could determine that the protections in R1 are therefore "not applicable" and not place any additional expectations on them?"

SCE&G believes the current language of R1 places unacceptable burden on the Regional Entities because the obligations of R1 occur at the end of the supply chain between Regional Entity and its vendor(s). Cyber security risks can occur at any phase of the supply chain(s) and R1 does not clearly demarcate the supply chain(s) where the risk management plan(s) apply. It is not clear how far in the supply chain(s) of a BES Cyber Asset do Responsible Entities need to identify and assess procurement risks. SCE&G is concerned that Regional Entities will be held responsible for assessment and mitigation of risks outside of the Entities' realm of influence over vendor internal processes and vendor's supply chain(s).

Likes 0	
Dislikes 0	

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

NRG recommends that the overall structure of the proposed CIP-013 standard be changed to be consistent with CIP-004 through CIP-011 standards (Specifically by applying similar formatting and use of applicability tables to identify the in-scope systems.) NRG recommends that the CIP-013 standard should focus only on R1 and R2. This would allow the operational controls to remain or be placed in the existing CIP standards.

NRG suggests that the drafting team consider the risk impact classification for Requirement R1 as they would with the other Requirements through the Standard. Additionally, we suggest the drafting team remove the phrase "if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" from the language of R1 and section 1.2 because, we think that this language is inconsistent with FERC Order 829 Directive language. Also, we suggest that the drafting team adds some clarity to the sub-parts of Section 1.2 on what are the SDT intentions for the industry in reference to these sub-parts.

In reference to R1 and contracts, NRG suggests that the term "future contracts" be addressed in the requirement language such as: "new or modified contracts" on or after the date of Enforcement. NRG recommends that these terms should be vetted in an implementation plan to include a conversation of initial compliance versus implemented/ongoing compliance (for example, Registered Entities need clear understanding of the scope as it pertains to plan reviews, new contracts, modified contracts, current contracts).

The Measurement and Requirement language is inconsistent with the sub-part language. In the second sentence of R1's Measures section, the term "mitigating" is used and we suggest replacing the term with "addressing". NRG recommends that the term "addressing" includes that Registered Entities have the flexibility to exercise all risk management options within a Risk Management Plan (to include an acceptance of risk).

Each requirement should have a provision that allows an entity to accept the risk of selection a vendor that will not or cannot supply a control. The requirement intent appears to be about control of a process of disclosure and communication (how a vendor notifies us). Whether a vendor fixes a vulnerability does not appear to be the direct scope or intent of the requirement. Therefore, obtaining specific controls in the negotiated contract may not be feasible. In these cases, NRG suggests that a failure to obtain and implement these

controls is not considered a failure to implement an entity's plan. NRG recommends that an entity be able to use a formalized risk management process to evaluate or accept the risk [Risk Management Plan]. In the event that a vendor cannot supply a control, that a Registered Entity may be able to present a mitigating control or that the Registered Entity be allowed to decide to accept the risk (for example a process to vet through a Registered Entity risk management, supply chain, and/or senior management departments and a process to accept risk based on a risk matrix). This may be implied by R1.2.7; however NRG recommends that the standard explicitly communicate that a level of risk acceptance can be part of an entities' Risk Management Plan. The Risk Management Plan could include steps to keep track of failures and steps to take in the event that vendor controls are found to be insufficient (for example, lessons learned feedback and correction process) - in the Measures section. An example of demonstration of compliance could be a periodic (i.e. 15 month) survey to the vendor during plan review (i.e. 15 month) validation of the notification processes between the two parties or dependent on the level or risk. NRG recommends that R1 should have a description of elements of a good Risk Management Plan (Measures) to include how deficiencies will be addressed, regular feedback to the vendor, and potential implications of non-conformance. NRG requests clarity on how revisions to the Risk Management Plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

For R.1.2.7, NRG recommends using "or" vs "and" after R1.2.6

In R1.2, NRG recommends rewording the requirement to "implement processes that describe controls to address risks identified in R1.1." NRG recommends that the intent of R1 to be to provide processes (for disclosure and responding controls). Therefore, NRG recommends that the Measure be limited to the sufficiency of the Entities' vendor controls and evaluation process. The Measures should state that the evaluation would be on an entities process for evaluation and if a vendor does not uphold a negotiated communication process, this does not reflect a compliance violation on the Registered Entity.

Likes 0	
Dislikes 0	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

1. The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined.

2. It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3. R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

4. For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5. For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6. For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list “planning, acquisition and deployment” and versions of these terms in the diagram. R1.1 uses “planning and development”. The meaning of “development” has not been clarified and is not part of the process addressed by this standard. Suggest that “development” be clarified or removed.

7. For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

   i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

   ii. To evaluate the effectiveness of mitigating that risk? or;

iii. Is it meant to identify the controls in place to mitigate the identified risks?

8. For R1.2.1: The words “Security Event” are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then” Security Event” should be replaced or clarified in the Requirement. This clarification could include “any identified, threatened, attempted or successful breach of the vendor’s components, software or systems used in the support of the Entity’s BES Cyber System.” This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3

9. For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

10. For R1.2.2: The requirement for the” process for notification” is very different than the “request vendor cooperation” guidance given on page 6, line 22 of the guidance document the requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that “A failure of a vendor to follow a defined process is not a violation of this Requirement.”

11. Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk

12. Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1

13. The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

“Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

“Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	

Same as RoLynda Shumpert's comments from SCE&G:

In addition to high and medium impact BES Cyber Systems, the applicability of R1 should be clear to include low impact BES Cyber Systems.

SCE&G agrees with the concerns and question raised by the Security Practices Working Group of North American Generator Forum (NAGF) regarding "if applicable":

"The phrase "if applicable" is ambiguous in the language of the main requirement. One reading is that "if applicable" means that the requirement only applies should the device types of associated EACMS, PACS or PCAs actually exist. Another reading is that "if applicable" is based on the risk that an entity places on a particular vendor as part of its documented risk management plan(s). If an entity performs a risk assessment of its vendors and finds that a vendor is a low or potentially zero risk (coupling a vendor's reputation with their particular usage within an entity), does this mean that an entity could determine that the protections in R1 are therefore "not applicable" and not place any additional expectations on them?"

SCE&G believes the current language of R1 places unacceptable burden on the Regional Entities because the obligations of R1 occur at the end of the supply chain between Regional Entity and its vendor(s). Cyber security risks can occur at any phase of the supply chain(s) and R1 does not clearly demarcate the supply chain(s) where the risk management plan(s) apply. It is not clear how far in the supply chain(s) of a BES Cyber Asset do Responsible Entities need to identify and assess procurement risks. SCE&G is concerned that Regional Entities will be held responsible for assessment and mitigation of risks outside of the Entities' realm of influence over vendor internal processes and vendor's supply chain(s).

Likes 0	
Dislikes 0	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	

With Vectren's commitment to safety, reliability, and compliance excellence, we appreciate the opportunity to provide comments. Vectren supports attention to the threat of inadequate supply chain risk management procedures and offer these comments to that end. We propose the SDT modify standard language based on Vectren's proposed language below:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to industrial control systems project planning that include processes to identify and evaluate risks during the procurement process. For control system procurement activities related to industrial control systems covered by NERC CIP Standards CIP-002 through CIP-012 and CIP-014 that shall include:

1.1 Planning, including the implementation of controls to identify, evaluate, and assess risks during the procurement and deployment of products and services.

1.2 Criteria for products and services that address:

1.2.1. Disclosing known product vulnerabilities;

1.2.2. Verifying product integrity and authenticity of software patches; and

1.2.3. Controlling vendor-initiated interactive remote access and machine-to-machine remote access.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R1

1.2 - How do we address these requirements with large companies (Microsoft, Oracle, etc.)? How do we document the decision to stay with a preferred source that refuses to comply or cannot comply? Is there a threshold or risk level?
1.2.1 - "Vendor security events" is too broad of a statement. Does this include physical security events as well? Vectren recommends placing some type of a boundary around this statement. How do we document the decision to stay with the vendor if they refuse to comply? Is this identifying for 1.2.4 coordination? How does vendor security event relate to vendor-related cyber security incidents – is it the same?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement of products, not operation/maintenance.
1.2.4 - "vendor-related cyber security incidents" is too broad of a statement. Place some type of a boundary around this statement. Coordinate with vendor, internally, what is our responsibility? If Microsoft has a phishing attempt, what does that mean to the utility? Is that an event for the utility? What is the trigger for the utility to implement their plan?
1.2.6 - Would an Entity-owned anti-virus server that provides signature updates to assets be considered "vendor initiated" system-to-system remote access?
Add the forward-looking language to the standard, itself.

Propose to remove security events. Would this require contract language that requires vendor to notify utility within 24 hours of a security event?

Likes 0	
Dislikes 0	
Richard Vine - California ISO - 2	

Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	

1) The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined.

2) It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3) R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

4) For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5) For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." This should be incorporated into the Requirement itself.

6) For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list "planning, acquisition and deployment" and versions of these terms in the diagram. R1.1 uses "planning and development". The meaning of "development" has not been clarified and is not part of the process addressed by this standard. Suggest that "development" be clarified or removed.

7) For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

{C}a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

{C}b. To evaluate the effectiveness of mitigating that risk? or;

{C}c. Is it meant to identify the controls in place to mitigate the identified risks?

8) For R1.2.1: The words "Security Event" are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then "Security Event" should be replaced or clarified in the Requirement. This clarification could include "any identified, threatened, attempted or successful breach of the vendor's components, software or systems used in the support of the Entity's BES Cyber System." This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3

9) For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

10) For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document The requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a

failure to implement the process. Would like to see an additional statement in the requirement language that "A failure of a vendor to follow a defined process is not a violation of this Requirement." 11) Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?	
Likes 0	
Dislikes 0	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy believes requirement R1 should only be applicable to BES Cyber Systems and recommends removing the portion of the requirement in R1 and R1.2 that states "and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets". The FERC order is focused on "industrial control system hardware, software, and services associated with bulk electric system operations" and does not mention Electronic Access Control and Monitoring System (EACMS), Physical Access Control System (PACS), or Protected Cyber Assets (PCA). These additional systems are low risk and not considered industrial control systems. CenterPoint Energy recommends taking a risk-based approach as stated in the FERC order, so entities can focus their efforts on the supply chain risk management of BES Cyber Systems, which pose a higher risk to the Bulk Electric System. Additionally, this requirement is applicable to High, Medium, and Low Impact BES Cyber Systems, but Low Impact BES Cyber Systems do not have EACMS, PACS, and PCA. If the intent of R1 is address the procurement controls, CenterPoint Energy recommends stating that in the main R1 requirement; otherwise, the sub-requirements in R1 can appear to be duplicative of the technical operational controls in R3 and R4. Furthermore, the expectation for R1 is not clear for open source products with no vendor or products bought off the shelf with no purchase contract.	

CenterPoint Energy recommends deleting R1.1.2 as the items in R1.2 appear to be the mitigation for the risks identified in R1.1. There is no need for a separate statement about mitigation in R1.1.2.

R1.2.1 uses the term “security events” which is not defined and the meaning could vary for each vendor. CenterPoint Energy recommends defining the term for consistency.

R1.2.2 appears to be redundant to CIP-004 R5.1 and R5.2 and extends to PACS and PCA requirements formerly required only for BES Cyber Systems (BCS) and Electronic Access Control and Monitoring Systems (EACMS).

R1.2.4 should capitalize the term “cyber security incident” because it is a NERC defined term.

R1.2.5 includes “all software and patches” which conflicts with the existing CIP Standards.

R1.2.6 is either redundant with or in conflict with CIP-005 requirements to identify inbound and outbound access permissions with reason for access and control remote access with 2 factor authentication and an identified access control system. It is unclear what additional evidence would be expected to satisfy this requirement.

R1.2.7 is far too broad, requiring and exposing to audit a potentially infinite number of new processes. The requirement wording is not appropriate for a Reliability Standard.

Likes 0	
Dislikes 0	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	

I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.

Likes 0	
Dislikes 0	
Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	

OUC has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

OUC does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, OUC requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, OUC believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, OUC requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

OUC requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

OUC is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see OUC’s response to Question #9 for additional information on exceptions).

OUC notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 OUC requests changing the word *evaluate* to *determine.*

For R1.2.1 OUC requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 OUC requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. OUC requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

Likes 0	
Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	

At the main Requirement level, while the rationale for Requirement R1 clearly states,

"Implementation of the cyber security risk management plan(s) ***does not require*** *the Responsible Entity to renegotiate or abrogate* ***existing contracts****, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan",*

the requirement language is silent to this stipulation and therefore could lead to future confusion if left absent from the requirement language.

For ultimate clarity, ATC recommends the SDT consider the inclusion of language within the Requirement R1 itself that provides this specificity of scope. Proposed language for consideration could include phrasing like, but not limited to:

"Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) for ***new/future vendor/supply chain contracts, agreements, and/or relationships*** *that address controls for mitigating…"*

Additionally, it is not uncommon for operational technology to be proprietary, and as such to limit the supplier base and/or the industry's options/bargaining power over supplier practices. While the Rationale provided by the SDT carries the message that the intent is for this requirement to be forward-thinking and exclude existing contracts, even if the above proposed language were incorporated for clarity, it does not address the gap incurred after initial enforcement and implementation is achieved. Once the Standard would be enforceable, inevitably existing contracts will continue to age and will need to be renewed or renegotiated. This requirement language does not address that condition, the feasibility of the imposed obligations upon the future expiration of existing contracts, nor the potential unintended consequences that may be incurred at the time that renewal or renegotiation process are initiated as those existing contracts reach maturity and ultimately expiration. Consequently, the industry must assure that any future regulations regarding supply chain are constructed in a manner that 1.) supports successful and ongoing accomplishment of safe, secure, resilient, and reliable operation of the Bulk Electric System as existing contracts reach maturity and inevitably age to the level of expiration, 2.) prevents the unintended consequences that are at variance with the intent to maintain safe, secure, resilient, and reliable operation of the Bulk Electric System.

As an example, some unintended consequences could include, and may not be limited to:

- Rendering previously contracted and necessary suppliers inviable upon the renewal or renegotiation of expiring/expired contracts creating a gap in the ability to procure necessary limited or proprietary supply that supports reliable operations,
- The industry being subject to the operationally risky, unnecessarily time-constrained, and cost prohibitive need to perform wholesale replacements of infrastructure with a new supplier to achieve compliance,
- The industry being held hostage by its suppliers through cost prohibitive supplier capitalization via unreasonable increase to the cost of supplier services containing contractual language that meet the CIP-013-1 requirements for their products/services.

The absence of a provision to accommodate for these potential conditions could lead to an impossibility of compliance and/or could compromise reliability if the Registered Entity 1.) cannot procure necessary products without being subject to a compliance violation, or 2.) is forced to abandon current solutions and perform wholesale upgrades or replacements of BES Cyber System infrastructure in order to comply, 3.) is forced to pay exorbitant fees to renegotiate/renew contracts with limited suppliers of necessary limited or proprietary products. Proposed language for consideration could include phrasing like, but not limited to:

"Each supply chain risk management plan(s) shall contain provisions to address instances where expired/expiring vendor/supply chain contracts, agreements, and/or relationships cannot be reasonably renewed in a compliant mode without posing significant risk to safe, secure, resilient, and reliable operation of the Bulk Electric System and its BES Cyber Assets."

Requirement R1:

The scope of R1 is too broad in its reference to BES Cyber Systems without consideration of impact-rating. Consequently, some of the proposed requirements are duplicative of existing requirements for high and/or medium impact BES Cyber Systems, and others exceed the controls required for approved and future enforceable CIP Cyber Security Reliability Standards for low impact BES Cyber Systems.

1. This approach is at odds with the overall intent for the CIP Cyber Security Standards to be constructed in a manner that applies graduated controls commensurate with the risk associated to the impact rating of the BES Cyber System.

2. This approach creates double jeopardy in certain instances, and is at variance with the approach to the body of documentation that comprises the CIP Cyber Security Standards wherein significant effort was invested to eliminate cross references and duplicative content.

3. Through it redundancy, this approach is at odds with the efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.

4. This approach is at odds with the directive in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard wherein "…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.

Requirement R1 Sub Requirement 1.1.2:

At the sub requirement level, R1 sub requirement 1.1.2 is broad and unclear. ATC recommends the SDT consider providing clarification if anything actionable is expected beyond just an evaluation, such as creating a plan to address the risk and then mitigating risk where possible.

Requirement R1 Sub Requirement 1.2.2:

R1.2.2 is simultaneously duplicative and additive to the language and/or intent of existing approved and effective CIP Cyber Security Reliability Standards as consequence of the broad reference to BES Cyber Systems without consideration of impact-rating in Requirement R1.

1. CIP-004-6 R4 and R5 address access management and revocation for **individuals** having cyber or unescorted access to specified high and/or medium impact-rated BES Cyber Systems and associated Cyber Assets. The existing enforceable CIP-004-6 standard is silent to the capacity with which a given individual is engaged with a Registered Entity, and therefore in its silence addresses employees, contractors, interns, apprentices, and even vendors or suppliers etc. The existing implemented access requirements within CIP-004-6 are more prescriptive than what is proposed for CIP-013-1 rendering CIP-013-1 R1.2.2 superfluous. Consequently, CIP-013-1 R1.2.2 adds no value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-004-6 R5. Through it redundancy, this approach is also at odds with the efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.

2. CIP-003-6 R1.2 prescribes policy level controls, and CIP-003-6 R2 Attachment 1 Sections 2-3 necessitate plans for the implementation of physical and electronic controls for low impact BES Cyber Systems. CIP-013-1 R1.2.2 effectively expands the scope and requirements for access of vendor employees beyond what is mandated as access requirements of low impact BES Cyber Systems to all other types of employees and Registered Entity engagements wit personnel. Any expansion in scope to access requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

3. Additionally, the inclusion of “onsite access” within the proposed language in 1.2.2 is an expansion in scope from the **second directive** in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard that “…should address the following security objectives, discussed in detail below: (1) software integrity and authenticity; **(2) vendor remote access**; (3) information system planning; and (4) vendor risk management and procurement controls.”

Requirement R1 Sub Requirement 1.2.4 and 1.2.6:

For consistency with other 1.2.x sub requirements, ATC recommends the SDT consider replacing 'Coordination' with 'Process' by revising the language in both R1.2.4 and R1.2.6 to "**Process** to respond to vendor-related….", and "**Process** to implement remote access controls…", respectively. **Requirement R1 Sub Requirement 1.2.5**: CIP-013-1 R1.2.5 is heavily dependent on supplier capabilities and their willingness to provide tools and/or mechanism to enable Registered Entities to perform integrity or authenticity verification. ATC recommends the SDT consider incorporating language that provides flexibility where it is not technically possible.	
Likes 0	
Dislikes 0	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	

Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	

1. We are concerned about the risks associated with BES Cyber Asset products and services that may contain potentially malicious functionality, are counterfeit, or are otherwise vulnerable due to poor manufacturing and development practices within the industrial control system supply chain. However, the proposed draft standard extends well beyond software authenticity and beyond the ability for entities to manage.

2. New requirements for notification of changes in supplier workforce and incident reporting are impossible to implement and audit due to a lack of a consistent approach and application amongst entities. Industry and industrial supply chain vendors would serve more time sending out notification agreements and attestations than working on making a better and more secure product. Would the supply chain vendor be required to send out a notification every time an employee leaves or finds a virus in the office? If so, then the requirement will be too burdensome for vendors and entities to manage.

3. We believe NERC language in the in the draft standard would have a significant negative impact on the industrial control system community over the long term. As seen in the nuclear industry, specific standards that are outside of other critical sectors will only drive cost up and a willing supply of vendors, down.

4. The need for such a broad set of requirements are unnecessary due to the existing requirement for the entity to have an incident response plan, anti-virus protection and patch management.

5. The additions of *"and, if applicable,* 4 *associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and* 5 *Protected Cyber Assets" in requirement 1 greatly expands the scope of cyber assets.* ACES recommends limiting the cyber assets in scope to BES Cyber Assets.	
Likes 0	
Dislikes 0	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the Cyber Security Supply Chain Management Technical Conference on November 10, 2016.

As part of Supply Chain Risk Management, Reclamation understands that the risks associated with interaction with vendors, their products, and/or their services are to be considered and mitigated with controls such as contract clauses, physical controls, and/or electronic controls (including vendor remote access). Reclamation recommends that Requirement R1 should instead address the development of one or more supply chain risk management plans that identify risks and controls for mitigating cyber security risks throughout the life cycle(s) of BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Within Requirement R1, the life cycle steps to consider in identifying risks and the respective controls should include but not be limited to: evaluation of design, procurement, acquisition, testing, deployment, operation, and maintenance.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Rationale for Requirement R1:

The rationale language for R1 states, “The cyber security risk management plan(s) specified in Requirement R1 apply to BES Cyber Systems." If the intent of the “BES Cyber Systems” reference is to be applicable for all three impact classifications (High, Medium and Low), IPC recommends adding impact classification language.

The rationale language for R1 states, “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.” How does the SDT expect Responsible Entities to demonstrate compliance if existing contracts are acceptable?

The rationale language for R1 states, “The objective of verifying software integrity and authenticity (Part 1.2.5) is to ensure that the software being installed in the applicable cyber system was not modified without the awareness of the software supplier and is not counterfeit.” How does the SDT expect Responsible Entities/vendors to demonstrate compliance with this?

The rationale language for R1 states, “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan." IPC suggests including the verbiage “with vendors, suppliers or other entities executed as of the effective date of CIP-013-1” to the third paragraph of the “Rationale for Requirement R1.”

R1

The requirement language for R1 states, "Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated EACMS, PACS and PCAs." If the intent of the "BES Cyber Systems" reference is to be applicable for all three impact classifications (High, Medium and Low), IPC recommends adding impact classification language. In addition, if the intent of the "if applicable" reference is to imply "EACMS, PACS and PCAs associated with BES Cyber Systems," IPC recommends replacing the "if applicable" language with "and their associated" language to remain consistent with current enforceable standard language.

R1.2 – IPC has concerns about the ability of a Responsible Entity to comply with, as written, R1.2, specifically R1.2.1 – R1.2.7. IPC believes there will be instances when vendors (e.g., larger IT vendors, smaller vendors, open source software, etc.) will not agree to provide all of the information necessary to meet the R1.2.1 – R1.2.7 requirements, potentially forcing Responsible Entities to look at other, lower quality options to ensure compliance, or vendors will use the required compliance control(s) as leverage during contract negotiations. The rationale for R1 states, "Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan." However, the rational language does not translate to a release from the R1.2 requirements. How does the SDT foresee Responsible Entities demonstrating compliance when an entity is unable to obtain a specified control(s)? Further, how does the SDT foresee these requirements being measured by auditors?

R1 and R1.2 require the development and implementation of "processes" and/or "plans." If vendors refuse to agree to terms, what implementation evidence does the SDT expect Responsible Entities to provide? Additionally, if the vendor agrees to the terms stated but fails to deliver according to the documented process, does the SDT foresee this being viewed as non-compliance?

IPC would like to know what additional security measures R1.2.1, R1.2.3, and R1.2.4 provide that aren't already covered by CIP-007-6, for example CIP-007-6 R2?

IPC recommends adding mitigation plan verbiage to R1.2 requirement language.

M1

The measure language for R1 states, "Evidence shall include (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk management

plan(s).” How will this measure apply to Responsible Entities who do not renegotiate or abrogate existing contracts or are unable to obtain specific controls?	
Likes 0	
Dislikes 0	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Santee Cooper does not agree with including all BES Cyber Systems in Requirement R1 and suggest using a risk-based approach, to limit this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Santee Cooper believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, Santee Cooper requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Santee Cooper requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

Santee Cooper is concerned about compliance obligations for procurement activities associated with system integrators. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they

provide important negotiating strength, flexibility, and effectiveness in contracting (see Santee Cooper's response to Question #9 for additional information on exceptions).

Santee Cooper notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used. Additionally, Santee Cooper requests that the term be used consistently throughout the standard and not switch between vendor and supplier.

For R1.1.2 requests changing the word *evaluate* to *determine.*

For R1.2.1 Santee Cooper requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. Santee Cooper requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

In Measure M1, Santee Cooper requests that the language be changed to be consistent with the Requirement. Specifically, change "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…" to "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…" (BOLD emphasis added). The construction "address risk" conforms to the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as opposed to mitigated.

Santee Cooper requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.

Likes 0	

Dislikes 0	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, LCRA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, LCRA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.	
Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes CIP-013-1 R1 should only apply to High and Medium cyber systems. Applicability to Low systems would potentially place a large burden as current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. BPA requests that the SDT provide clarification as to how R1 would apply to TCAs.	

1.2.1 - Is notification under 1.2.1 for what is known at the time of procurement or does it persist after the procurement is fulfilled? What is the time limit? BPA proposes that the language be made consistent with the R1 rationale: “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

1.2.2 through 1.2.6 – BPA believes this expands the scope of CIP-004 R5. BPA requests clarification on what this applies to: does it apply to the vendor or to the hardware/software?

The SDT should address gaps that apply to other standards within that standard and not group them into CIP-013-1. For the sub-parts of CIP-013 R1, the scope might be more appropriate in the following locations:

- The topic of access control CIP-013 R1, P1.2.2 is addressed in CIP-004 R5, P5.1
- Vulnerability assessments CIP-013 R1, P1.2.3 is addressed in CIP-010 R3, P3.1
- Cyber security response CIP-013 R1, P1.2.4 is addressed in CIP-008 R1, P1.1
- Software security patches CIP-013 R1, P1.2.5 is addressed in CIP-007 R2, P2.1-2.4; BPA suggests revision to address all patches.
- Interactive Remote Access CIP-013 R1, P1.2.6 is addressed in CIP-005 R2, P2.1.

Likes 0	
Dislikes 0	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) The Rational for Requirement R1 includes a definition of the term "vendors". This definition is also included in the Guidelines and Examples document. This term should be officially defined in the standard or added to the NERC Glossary of Terms and capitalized when used.

2) For R1: This requirement requires both the development and the implementation of a plan. We recommend modifying this requirement into three steps which follows the CIP-014 structure – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline. The timeline should use fixed dates or intervals and not dates that are linked to the completion of other compliance activities

3) The standard as written addresses Vendor Risk Management and no other supply chain risks such as sole source and international dependencies. Suggest changing the name, purpose, and other areas of the standard from supply chain" to "vendor".

4) For R1.1.2:

a. We recommend changing *evaluate* to *Determine.* We also seek further clarification of the intent. As, written the requirement is ambiguous:

i. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

ii. to evaluate the effectiveness of mitigating that risk? or;

iii. is it meant to identify what controls you have to mitigate the risks you have?

b. The evaluation of methods is a administrative task and similar to other tasks removed from the NERC standards as part of the Paragraph 81 project.

5) For R1.2.1: The words "Security Event" are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then this should be an officially defined term either in the standard or in the NERC glossary. The s definition provided in the glossary is "any identified, threatened, attempted or successful breach of vendor's components, software or systems" and "that have potential adverse impacts to the availability or reliability of BES Cyber Systems" It is unclear if the second portion is meant to be part of the definition. Many cyber systems, like firewalls, are under constant threat and attempts to breach the systems security. Suggest replacing "vendor security event" with "identification of a new security

vulnerability". Vendors may not be able to determine if a vulnerability "could have potential adverse impact to the availability or reliability of BES Cyber System". This clause would only be applicable in determining when an entity would notify a vendor.

6) For R1.2.1: Page 6, line 12 of the Guidance and Examples document list both notification of security events from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both types of notifications.

7) For R1.2.1: The requirement for the" process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document.

8) Page 6, line 12 of the guidance details the notification of the vendor by the entity. It is unclear that the R1.2.1 requires notification by the entity to the vendor as detail in the guidance document.

9) Recommend that "Security Event" be changed to require the reporting of only newly identified security vulnerabilities.

10) Change 1.2.7 from pointing to 1.1.2 to 1.1.1. Remove 1.2 since 1.2.7 covers 1.2.

11) Do not agree with the current draft language that includes all High, Medium and Low BES Cyber Systems in Requirement R1. Suggests limiting this requirement to High and Medium only as the current Low Impact requirements do not require entities to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. If controls are needed for low impact, suggest moving these to R5 to consolidate all low impact into a single requirement.

12) The Standard drafting team needs to verify that the SDT needs to make sure that there is no duplication in the standards. Provide guidance on how areas that seem to overlap like Interactive Remote Access and CIP-005.

13) Request the SDT to consider adding the following language from the rationale to the language of the standard "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

14) The Rationale for R1, it states that R1, P1.1 addresses P 56 of Order No. 829. P 56 calls for a risk assessment of the entities internal systems with this language "how a responsible entity will include security considerations as part of its information system planning and system development lifecycle processes". R1, P1.1.1 calls for a risk assessment of the vendors systems with this language "procurement and

deployment of vendor products and services." The language in the order does not match the language in the standard and therefore suggest that the language be consistent to provide clarity. 15) There could be an impact of contract requirements on the ability of public utilities to piggyback on wide-area contracts such as those of National Association of State Procurement Officials (NASPO) Cooperative, Western States Contracting Alliance (WSCA), Washington State Department of Enterprise Service, and others. Recommend that an exclusion be permitted in the case of such contracts, which are important to provide flexibility, effectiveness, and negotiating strength for public utilities throughout the country. In some cases such contracts are required; also include language that provides an exclusion for contracts that are covered by other laws or regulations. 16) The measure should not reference the word mitigation, which to an auditor may limit the actions an entity might take to address risk (such as avoid or transfer). Suggest that "mitigate" be replace with "address" as listed in R1.2.	
Likes 1	Austin Energy, 3, Preston W. Dwayne
Dislikes 0	
Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No

Document Name	
Comment	
The FERC order applied to industrial control systems. The SDT is applying the standard to all BES Cyber Assets or systems. It is our belief that all BES Cyber systems are not industrial control systems. The SDT should apply the requirements to industrial control systems such as DCS or EMS systems located in power plants and control rooms.	
Likes 0	
Dislikes 0	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Colorado Springs Utilities (CSU) has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives. CSU does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, CSU requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, CSU believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, CSU requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.	

CSU requests that the SDT add the following language from the rationale to the language of the standard: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

CSU is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see CS's Uresponse to Question #9 for additional information on exceptions).

CSU notes that the Rationale for R1 includes a definition of the term “vendors”. This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 CSU requests changing the word *evaluate* to *determine.*

For R1.2.1 CSU requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 CSU requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the “process for notification” which is very different than the “request vendor cooperation” language. The requirement as written would require that a process be defined and implemented. CSU requests additional language in the requirement that addresses “entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement.”

In Measure M1, CSU requests that the language be changed to be consistent with the Requirement. Specifically, change “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…” to “Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…” (BOLD emphasis added). The construction “address risk” conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as opposed to mitigated.

CSU requests that the title of the standard be changed to “Vendor Risk Management” to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term “supply chain risk management” encompasses a much

broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.	
Likes 0	
Dislikes 0	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The Rationale for R1 states, “Implementation of elements contained in the entity’s plan related to Party 1.2 is accomplished through the entities procurement and negotiation process.” The SDT need to define the process for determining the minimum level deemed to be sufficient. Additionally, the SDT needs to identify the course of action an entity must take and document where a vendor is unwilling or unable to meet the obligations set forth for Responsible Entities.

R1. In FERC Order No. 829, paragraph 59 states, “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.” The Order does not address requirements for EACMS, PACS, or PCA as identified in R1. The SDT should limit the requirement to the context of the Order.

R1.1.1. The obligation to “identify and assess risks” is extremely open-ended and ambiguous. In contrast, the draft Technical Guidance and Examples document enumerates a list of 11 factors that should be considered in an entity’s plan. NERC standards should be clear on their face, and it is inappropriate to require and entity to refer to draft Technical Guidance and Examples document for fundamental questions concerning whether an entity is compliant with a given requirement. If the Drafting Team believes that this list of 11 factors within the draft Technical Guidance and Examples document is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe

this list is complete or appropriate, an alternate list of factors should be provided. Without clear requirements on the factors to be considered, there is substantial risk in inconsistency of implementation by entities. R1.1.1. The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production. To avoid confusion, the term “deployment” should be removed.	
Likes 0	
Dislikes 0	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx
Comment	

The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.

Seattle City Light has been engaging in dialogue with peers of trade associations such as Large Public Power Corporation to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives.

Seattle City Light does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, Seattle City Light requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of equipment and software or identify systems, Seattle City Light believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of

requirements to address their lower risk, Seattle City Light requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

Seattle City Light requests that the SDT add the following language from the rationale to the language of the standard: "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

Seattle City Light is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as national, regional, state & city negotiated contracts. Examples include contracts from the National Association of State Procurement Officials (NASPO) Cooperative and the Western States Contracting Alliance. In some cases use of these contracts in procurement is mandated by other laws or regulations. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities because they provide important negotiating strength, flexibility, and effectiveness in contracting (see Seattle City Light's response to Question #9 for additional information on exceptions).

Seattle City Light notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 Seattle City Light requests changing the word *evaluate* to *determine.*

For R1.2.1 Seattle City Light requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 Seattle City Light requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. Seattle City Light requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

In Measure M1, Seattle City Light requests that the language be changed to be consistent with the Requirement. Specifically, change "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for MITIGATING cyber security risks as specified in the Requirement…" to "Evidence shall include (i) one or more documented supply chain cyber security risk management plan(s) that address controls for ADDRESSING cyber security risks as specified in the Requirement…"

(BOLD emphasis added). The construction "address risk" conforms with the text of the Requirement and acknowledges that risk might be avoided or transferred, for example, as alternatives to being mitigated. **Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk. A change of title is a simple means to clarify what is intended in R1.1, in particular, and helps identify auditable actions throughout R1.**	
Likes 0	
Dislikes 0	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4;	

Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
It is unclear how the risk and requirements in R5 for Low Impact BES Cyber Systems are differentiated from the other requirements and how the requirements will be measured considering a list of Low Impact systems are not required. There seems to be some reduncancy between R1 and R5 for Low Impact. Suggest removing Low Impact requirements from CIP-013 and incorporating into CIP-003 for consitency.	
Likes 0	
Dislikes 0	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	

Comment

Ambiguity in R1

FERC Order No. 829 asks for a plan to be developed and implemented by the entity that **includes** security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. It recognizes the diversity of BES Cyber System environments, technologies and risks among entities. FERC states that the "Reliability Standard may allow a responsible entity to meet the security objectives discussed below by having a plan to apply different controls based on the criticality of different assets."

We find that the use of word "address" in R1 is creating ambiguity.

We suggest that requirement should be clear in stating that entities are to identify supply chain cyber security risks, evaluate controls and select controls, and implement controls based on their acceptable risk levels for future procurement contracts.

In doing so, entities should consider, at minimum, the controls that are itemized in the FERC Order and evaluate whether implementation of those controls are appropriate based on risk.

The four objectives that R1 should address are not clear

FERC Order states the "following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., 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"))."

The required plan is not tied to the objectives stated in the FERC Order.

1. For Information System Planning, FERC Order appears to ask that the responsible entity must include security considerations as part of its information system planning and system development lifecycle. The information system planning and development lifecycle should be periodically reviewed and approved by CIP Senior Manager.

We believe that R1.1 is intended to address the Information System Planning objective in the FERC Order. Consideration of security risks in Information System Planning is the objective of the overall plan.

R1.1 causes ambiguity. It is not clear how controls can be used to identify and assess risk. Controls are used to mitigate risk. Evaluation of controls is performed prior to their selection depending on the acceptable level of risk and cost associated with the controls. The verbiage of Part 1.1.2 requires controls for the evaluation of methods to address risks. It does not require risks to actually be determined.

2. R1.2 lists a number of controls (some specifically stated in the FERC Order) and does not identify which objective these controls are to address.

a. For Software Integrity and Authenticity objective, FERC Order appears to ask that at minimum, entities should consider implementing the following controls to mitigate risk by:

1. Verifying the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and

2. Verifying the integrity of the software and patches before they are installed in the BES Cyber System environment. (R1.2.5)

The Standard appears to address this objective in Requirement 3. There is overlap/redundancy between R1.2.5 and Requirement 3.

b. For Vendor Remote Access to BES Cyber Systems, FERC Order appears to ask that at minimum, entities should consider implementing controls to mitigate risk by Logging and controlling all third-party (i.e., vendor) initiated remote access sessions including user-initiated and machine-to-machine vendor remote access. (R1.2.6)

The Standard appears to address this objective in Requirement 4. There is overlap/ redundancy between R1.2.6 and Requirement 4.

c. For Vendor Risk Management and Procurement Controls, FERC Order appears to ask that at minimum, entities' controls should consider implementing controls to mitigate by means of:

1. Vendor security event notification processes; (R1.2.1)

2. Vendor personnel termination notification for employees with access to remote and onsite systems; (R1.2.2)

3. Product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; (R1.2.3)

4. Coordinated incident response activities; and (R1.2.4)

5. Other related aspects of procurement. (R1.2.7)

Related to R1.2.1, It is not clear what constitutes a "vendor security event". Every vendor may have a different consideration for what constitutes a "security event". It could include an instance of employee fraud, workplace assault, or even the announcement of a patch release.

Related to R1.2.4, Cyber Security Incident is a NERC defined term. Is a cyber security incident a Cyber Security Incident? If not, what is the distinction? If it is, the term will need to be capitalized. Also the term "vendor related cyber security incident" is not clear. Is it a Cyber Security Incident that could happen during procurement and deployment stage?

We also find R1.2.7 is unnecessary and creates ambiguity.

Applicability

FERC Order suggests that entities can perform their own assessment of risks and determine applicability of controls based on that.

It is not clear how the described controls are applicable to BES Cyber Systems based on their risk level in the context of CIP Standards (Low, Medium, and High).

The Standard extends applicability to the EACMS, PACS, and PCAs associated to BES Cyber Systems. We argue that PACS, EACMS and PCAs, although are important for Physical and Electronic Security, are not necessarily "industrial control system hardware, software, and computing and networking services associated with bulk electric system operations" as stated in the FERC Order.

This standard should not be applied to systems or assets not needed for BES operations.

Likes 0	

Dislikes 0	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	
The NYPA Comments	
Likes 0	
Dislikes 0	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
Sacramento Municipal Utility District (SMUD) has been engaging in dialogue with peers of trade associations such as Large Public Power Council to address the CIP-013 standard development activities. We continue to be a strong supporter of efforts that ensure the security of the bulk electric system. We appreciate the great strides that the SDT has made in the development of this standard to address the elements of the FERC Order while balancing reasonable responsibilities as required by the electric industry in support of the security objectives. SMUD does not agree with including all BES Cyber Systems in Requirement R1. SMUD supports a risk-based approach, while limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of	

equipment and software or identify systems, SMUD believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, SMUD requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.

SMUD requests that the SDT add the following language from the rationale to the language of the standard: "Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

SMUD is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts such as state & city negotiated contracts. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities (see SMUD's response to Question #9 for additional information on exceptions).

SMUD notes that the Rationale for R1 includes a definition of the term "vendors". This definition is also included in the Technical Guidance and Examples document. This term should be officially added to the NERC Glossary of Terms and capitalized when used.

For R1.1.2 SMUD requests changing the word *evaluate* to *determine.*

For R1.2.1 SMUD requests that the words Security Event and the definition from the Technical Guidance and Examples document be placed in the NERC Glossary of Terms and capitalized when used.

For R1.2.1 SMUD requests that the SDT provide clarification on the language in the guidance document related to 1.2.1. The document references the "process for notification" which is very different than the "request vendor cooperation" language. The requirement as written would require that a process be defined and implemented. SMUD requests additional language in the requirement that addresses "entities are not required to validate a vendor is adhering to its processes and a failure of a vendor to follow a defined process is not a violation of this Requirement."

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Likes 0	

Dislikes 0	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

Requirement Placement (CIP-013 versus CIP-003)

R1 (and R2) includes low, medium, and high BES Cyber Systems; however, the current CIP Standards put the low impact BES Cyber Systems (LIBCS) requirements in CIP-003. EEI recommends that the SDT consider whether to move the LIBCS requirements from CIP-013 into CIP-003. Moving the LIBCS to CIP-003 may make it easier for Responsible Entities with only LIBCS to implement the requirements.

However, Responsible Entities with high, medium, and low impact BES Cyber Systems (HIBCS, MIBCS, and LIBCS) may be concerned that moving the supply chain LIBCS requirements to CIP-003 may make it difficult for them to take a holistic approach to the CIP-013 requirements. For example, some entities may want to focus on their BES Cyber System vendors and apply a single vendor-based approach for HIBCS, MIBCS, and LIBCS. Also, CIP-013 is focused on the risk that vendors and suppliers may introduce into BES Cyber Systems, whereas the other CIP Standards are focused on more general cybersecurity risks that can be addressed by Responsible Entity operational controls, which are within the control of the Responsible Entity. Third-party risk is harder for Responsible Entities to control and the methods of control are more likely contractual than operational. For example, a Responsible Entity cannot control a vendor's manufacturing process, but can ask questions during procurement as to how security risk is managed by the vendor to help evaluate the level of risk the vendor may pose to the Responsible Entity. As a result, there may be value in keeping these requirements out of the other CIP Standards, which focus on operational controls for cybersecurity risk.

Applicable Systems

Requirement R1 applies to LIBCS as well as HIBCS and MIBCS and their associated EACMS, PACS, and PCAs. We do not believe that EACMS, PACS, and PCAs should be included under the scope of Requirement R1. The diversity and sheer number of these systems make it difficult to

document how Responsible Entities will address procurement for all of these systems in their risk management plans. Auditing these plans will also be difficult.

Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor's product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement's objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using "industrial control systems associated with BES Cyber Systems" may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.

Security Objective

The security objective of Requirement R1 is unclear. Although it focuses on the Commission objectives 3 and 4, it would be helpful to make it clear in the requirement language so that Responsible Entities understand the purpose of the requirement.

Objective 3 is focused on making sure that Responsible Entities do not unintentionally plan to procure or fail to anticipate security issues during procurement or technology/vendor transitions. Objective 4 is focused on ensuring security concepts are addressed in future contracts. Both of these objectives are focused on evaluation of the risk that the vendor or vendor product/service may introduce to the BCS by the Responsible Entity during planning for and actual procurement of new systems. The controls that are required under Requirement R1 are also not operational controls, but process controls to assess and evaluate the risk.

Risk Acceptance

We understand that Order No. 706 ordered the ERO to remove acceptance of risk language from the CIP Reliability Standards. In this case, it was tied to a concern over uncontrolled compliance exceptions to addressing potential vulnerabilities and the Commission preferred the use

of technical feasibility, which led to technical feasibility exceptions. (See Order No. 706, P 150-151) We are not recommending the use of "acceptance of risk" in CIP-013, but we want to make it clear that risk acceptance may be a good option in dealing with procurement controls (CIP-013, Requirement R1), which are different than the operational controls covered by the other CIP Standards.

The security objective for Requirement 1 is focused on Responsible Entity awareness of risk that may be introduced by the vendor or vendor product/service. The Responsible Entity's ability to control this risk is limited. For example, the Responsible Entity may only have a few vendors to choose from for a particular procurement and the vendors may not have a well-defined process for vendor security event notification. The Responsible Entity can ask them to define a process and can even put language into a contract to require such a contract, but the vendors can say no. The Responsible Entity is left with the choice of either not procuring this device or system or accepting the risk. Documenting a compliance exception for every term the vendor does not agree to does not seem reasonable in light of the scope of Requirement R1 – the sheer numbers of systems covered (HIBCS, MIBCS, and LIBCS) and diversity of vendors for each of these systems and system components. Responsible Entities also cannot make the vendor develop or follow this process even if the vendor agrees to, which is also a consideration for the SDT – if the vendor does not comply with their contract terms is the Responsible Entity subject to a violation and penalty?

We recommend that the SDT consider, set, and articulate compliance expectations with Requirements R1 and R2 and recognize the difference between these procurement controls and the operational controls found in the rest of the CIP Standards.

Measure M1

We are concerned with the M1 language use of "written agreements" as a measure of plan implementation, even though it is introduced with "could include, but is not limited to." Requirement R1 does not (and should not) require Responsible Entities to use contract terms to meet the security objective. However, contract terms may be one method of "how" to meet the security objective ("what"), but not all entities will choose this "how". We are concerned that the inclusion of "written agreements" in the measure text suggests that this is a key piece of evidence for compliance with R1. Also, the use of "correspondence" in M1 could include "written agreements" if an entity chooses to use them for R1. We recommend removing "written agreements in electronic or hard copy format" from M1.

We recommend the following language for consideration by the SDT:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) to minimize the cyber security risks from vendors and vendor products and services to BES Cyber Systems during planning and procurement of industrial control systems. The plan(s) should address one or more methods to:

1.1. Raise awareness of risk the vendor and vendor product or service may introduce, including awareness of vendor process(es) to:

1.1.1. Notify the Responsible Entity of vendor security events;

1.1.2. Notify the Responsible Entity of when vendor employee remote or onsite access should no longer be granted;

1.1.3. Disclose known vulnerabilities to the Responsible Entity;

1.1.4. Coordinate the response to vendor-related cyber security incidents with the Responsible Entity;

1.1.5. Verify the software integrity and authenticity of vendor software and patches; and

1.1.6. Control remote access, including vendor-initiated interactive remote access and system-to-system remote access to the Responsible Entity

1.2. Assess risk(s) introduced by the vendor and vendor product or service identified by Part 1.1; and

1.3. Evaluate method(s) to address risk(s) identified by Part 1.2.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	

Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language. Particularly R1 should only focus on supply chain risk management during the procurement phase rather than controls during operations. Operational controls on BES systems should be covered in other CIP standards. Furthermore, if controls are to be required on a vendor's manufacturing process, in addition to those identified during RFP negotiations, these controls should be consistent and verifiable by an industry standard (similar to ISO(?) 9001 certification).	
Likes 0	
Dislikes 0	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA does not agree with including all BES Cyber Systems in Requirement R1. Using a risk-based approach, LCRA requests limiting this requirement to high and medium only. As the current low impact requirements do not require entities to conduct an inventory of	

equipment and software or identify systems, LCRA believes this requirement will place substantial additional administrative burden on entities with low impact assets. If a risk management plan is to be required low, with a reduced set of requirements to address their lower risk, LCRA requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Many of the aspects of CIP-013-1 R1 cannot be controlled by the entity, but instead need to have assurances from the vendor. In other CIP standards there are operational controls that the entity can make to meet the requirements of the standards; these controls are things the entity can control.

The scope of R1 includes BCAs, EACMS PACS and PCAs with no guidance concerning the risk associated with each of these types of assets. Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor's product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement's objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the

risk. For example, using “industrial control systems associated with BES Cyber Systems” may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.	
Likes 0	
Dislikes 0	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	

The IRC and SWG thanks the Drafting Team for their work and support the concepts in the security program enhancements addressing supply chain risks.

The Rationale for R1 states, “Implementation of elements contained in the entity’s plan related to Party 1.2 is accomplished through the entities procurement and negotiation process.” The SDT need to define the process for determining the minimum level deemed to be sufficient. Additionally, the SDT needs to identify the course of action an entity must take and document where a vendor is unwilling or unable to meet the obligations set forth for Responsible Entities.

R1. In FERC Order No. 829, paragraph 59 states, “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.” The Order does not address requirements for EACMS, PACS, or PCA as identified in R1. The SDT should limit the requirement to the context of the Order.

R1.1.1. The obligation to “identify and assess risks” is extremely open-ended and ambiguous. In contrast, the draft Technical Guidance and Examples document enumerates a list of 11 factors that should be considered in an entity’s plan. NERC standards should be clear on their face, and it is inappropriate to require and entity to refer to draft Technical Guidance and Examples document for fundamental questions concerning whether an entity is compliant with a given requirement. If the Drafting Team believes that this list of 11 factors within the draft Technical Guidance and Examples document is a comprehensive list of factors that should be considered when “identifying and assessing

risks," these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, an alternate list of factors should be provided. Without clear requirements on the factors to be considered, there is substantial risk in inconsistency of implementation by entities.

R1.1.1. The use of the term "deployment" can be read to require an ongoing obligation even after the software or hardware is in production. To avoid confusion, the term "deployment" should be removed.

Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Many of the aspects of CIP-013-1 R1 cannot be controlled by the entity, but instead need to have assurances from the vendor. In other CIP standards there are operational controls that the entity can make to meet the requirements of the standards; these controls are things the entity can control.

The scope of R1 includes BCAs, EACMS PACS and PCAs with no guidance concerning the risk associated with each of these types of assets. Some products and services may pose greater risk than others depending on many factors including risk introduced by the vendor, risk introduced by the vendor's product/service, or how the Responsible Entity deploys the vendor product or service. As a result, the requirement's objective should be to get Responsible Entities to evaluate vendor cybersecurity practices during procurement and develop methods to mitigate potential risks, whether that is choosing another vendor, implementing an operational control, or accepting the risk. CIP-013 cannot address all risk introduced by vendors and their products and services. Vendors have a responsibility to reduce risk in their manufacturing processes and Responsible Entities have a responsibility to reduce risk in their operations. The existing CIP standards already address Responsible Entity operational risk.

We are also concerned that by specifying the applicable systems in Requirement R1 that the requirement may be interpreted that every device in a system must be addressed by these plans. We recommend that the SDT consider either narrowing the scope of the requirement language or making it more flexible to allow Responsible Entities to define which systems need to be addressed by the plans based on the risk. For example, using "industrial control systems associated with BES Cyber Systems" may narrow the scope to more critical systems; however, industrial control systems would need to be defined by the SDT as interpretations may vary.	
Likes 0	
Dislikes 0	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

Q1-Issue1-Discussion

(1) In reviewing the measures M1, R1 is written in a manner to collect evidence to achieve two objectives; (i) documentation of the plan, and (ii) documentation to demonstrate implementation of the plan(s). According to NERC's Drafting Team Reference Manual which was recently revised and published October 19, 2016, on page 11 under section B – Requirements and Measures (http://www.nerc.com/pa/Stand/Resources/Documents/Drafting%20Team%20Reference%20Manual_Oct2016_final.pdf), each requirement should "achieve one objective." The Reference Manual goes on to state: *If a requirement achieves two objectives, such as developing a document and distributing that document, then each objective should be addressed in its own requirement.* Contrary to instructions delineated in the Reference Manual, R1 requires Entities meet two objectives, develop **and** implement the supply chain risk management plan.

Q1-Issue1-Recommendation

GTC recommends R1 be separated into two separate requirements where the first objective of the FERC directive identified in paragraph 2 is addressed to "develop a plan" (R1), and the second objective is addressed in its own requirement to "implement the plan" (new R2). This method simplifies compliance documentation for the Responsible Entity and aligns with the principles documented in NERC's Reference Manual. Additionally, this method will simplify and provide clarity to achieve FERCs directive for the plan to be forward-looking as explained in further detail below.

Q1-Issue2-DISCUSSION

(2) The SDT has clarified in the rationale for requirement R1 that the implementation of the cyber security risk management plans(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 as specified in the Implementation Plan. Additionally, Paragraph 59 stipulates to address security concepts in "future contracts". However, GTC does not see this forward looking language in the actual Requirement R1 that is specified by the FERC Order. GTC believes this forward looking language can be better clarified and highlighted if the SDT accepts GTC's first recommendation to separate R1 into two requirements and "implement the plan" is written as its own requirement.

Q1-Issue2-Recommendation

GTC recommends the following:

Separate R# to implement plan(s), then update the new Requirement with the following language: "Each Responsible Entity shall implement the documented supply chain risk management plan(s) specified in Requirement R1. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts."

Q1-Issue3-DISCUSSION

(3) Paragraph 45 of Order No. 829, clearly specifies "The Plan" should address, at a minimum, four specific security objectives in the context of addressing supply chain management risks.

(P. 45) The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Although R1 technically covers the four specific security objectives, the presentation lends itself somewhat confusing. R1.2.5 seems to align with security objective (1), R1.2.6 seems to align with security objective (2), and are both subsets to R1.2 which seems to align with security objective (4).

Q1-Issue3-Recommendation

GTC believes R1 will be clearer to understand and that the drafting team could gain more support if the four specific security objectives required by Order 829 Paragraph 45 had their own individual sub-requirement of "The Plan", in lieu of sub-requirements of one of the security objectives such as:

R1.1 aligns with security objective 3 (*information system planning*) where the specifics of the third objective identified in paragraph 56 is captured as a subset of R1.1;

R1.2 aligns with security objective 4 (*vendor risk management and procurement controls*) where the specifics of the fourth objective identified in paragraph 59 is captured as a subset of R1.2;

R1.3 to align with security objective 1 (*software integrity and authenticity*) where the specifics of the first objective identified in paragraph 48 is captured as a subset of R1.3; and

R1.4 to align with security objective 2 (*vendor remote access*) where the specifics of the second objective identified in paragraph 51 is captured as a subset of R1.4.

Q1-Issue4-DISCUSSION

(4) Order 829 Paragraph 58 refers to NIST Special Publication 800-53 for various supply chain development life cycle controls. The definition of Supply Chain from NIST SP 800-53 r4 states that the "supply chain horizon" ends at the delivery of products/services to the acquirer. FERC Order 829 acknowledges this definition in paragraph 32, footnote 61.

Supply Chain: “Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer”

Accordingly, in the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur “upon commissioning” for planned system installations (and even later for unplanned changes). Therefore, BES Cyber System identification, categorization as high, medium, or low impact; and also identifying associated EACMS, PACS, and PCAs does not exist during the supply chain context. Therefore, R1 should be limited to a supply chain risk management plan which will address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services of Cyber Assets which are intended to support Bulk Electric System operations as specified in Order 829 paragraph 43.

Q1-Issue4-Recommendation

GTC recommends the SDT adopt the aforementioned NIST SP 800-53 defined term Supply Chain for use with CIP-013-1 R1 in front of the term “risks” to contain the Time Horizon to supply chain risk management, and also edit to account for the fact that BES Cyber System identification and categorizations do not exist during the supply chain context.

An example of R1 is provided:

R1. Each Responsible Entity shall document a Supply Chain risk management plan(s) that address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services which are intended to support Bulk Electric System operations. The plan(s) shall address:

R1.1 The use of controls for mitigating Supply Chain risks associated with *information system planning*

R1.2 The use of controls for mitigating Supply Chain risks associated with *vendor risk management and procurement controls*

R1.3 The use of controls for mitigating Supply Chain risks associated with *software integrity and authenticity*

R1.4 The use of controls for mitigating Supply Chain risks associated with *vendor remote access*

Q1-Issue5-DISCUSSION

GTC disagrees with the inclusion of associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets in requirement R1. GTC finds no reference to the inclusion of these associated systems in FERC Order 829 and recommends their removal from this standard.

Further, GTC questions whether the use of the term BES Cyber Systems is appropriate in a standard which is limited per FERC Order 829 to "the context of addressing supply chain management risks." In the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur "upon commissioning" for planned system installations (and even later for unplanned changes). Therefore, BES Cyber System identification, categorization as high, medium, or low impact; and also identifying associated EACMS, PACS, and PCAs does not exist during the supply chain context.

Q1-Issue5-Recommendation

GTC recommends the removal of any reference to Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. GTC recommends removal of references to BES Cyber Systems and replacing it with the phrase "hardware, software, and computing and networking services which are intended to support Bulk Electric System operations."

Likes 0	
Dislikes 0	

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

R1.1 is acceptable in regard to requiring entities to have a plan to identify and assess risks with procured equipment. R1.2 is unacceptable because Entity creation of Detective Controls for the four Objectives of P. 45 is considered out of the Entity's scope. If only one Entity and one Vendor existed, the individual sub-parts of R1.2 may be feasible for control planning – but this approach is not viable for hundreds of

entities and dozens of vendors. The Entity is capable of identifying Preventative Controls, in concept, but they will only be effective if all the vendors in the supply chain make a diligent effort to implement the controls all the way back to the first-line suppliers. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified.	
Likes 0	
Dislikes 0	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
The requirement should focus on the risk of the software or services being procured and not allow for the possibility of a Registered Entity taking a risk view based upon the impact categorization of the BES Cyber System or EACMS, PACS, or PCA that is affected by the	

procurement. The requirement needs to clearly be focused on the vendor processes without regard to the Cyber Assets impacted by the vendor. The controls need to include processes for granting vendor access in addition to the processes for notifying when removal of access is necessary. The controls to grant access should include expectations for the conduct of training and personnel risk assessments, including review, modification as necessary, and acceptance of the vendor's process by the Registered Entity, if applicable, along with expectations of what evidence of compliance will be provided to the Registered Entity by the vendor. Part 1.2.4 should include an expectation of notification by the vendor in addition to coordination of the response.	
Likes 0	
Dislikes 0	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) The Rational for Requirement R1 includes a definition of the term “vendors”. This definition is also included in the Guidelines and Examples document. This term should be officially defined.

2) It is not clear if R1 applies to high, medium and low since R3, R4 and R5 specify the impact level. The high, medium, low impact level applicability would be much easier to understand if this standard were written to be consistent with CIP-004 through CIP-011 through the use of Applicability Tables.

3) R1.1 is vague in the language used with terms like “assess risk” and “evaluate”. The need to revise CIP-002 shows the difficulties that have occurred when entities are required to assess risk. Request that the SDT encourage NERC to include in the CIP-013 RSAW, language similar to that used in the CIP-003-7(i) RSAW, Attachment 1 Section 4, possible Notes to Auditor:

“The entity must document its determination as to what are the supply chain risks. Once this determination has been made and documented, the audit team’s professional judgement cannot override the determination made by the Responsible Entity. “

For R1: With respect to the obligation to “identify and assess risks,” the standard is extremely open-ended. In contrast, the Compliance Guidance enumerates a list of 11 factors that should be considered. NERC standards should be clear on their face, and it should not be necessary to refer to Compliance Guidance for basic questions concerning whether an entity is in compliance with a given requirement. If the Drafting Team believes that this list of 11 factors is a comprehensive list of factors that should be considered when “identifying and assessing risks,” these factors should be listed in the standard as the exhaustive set of factors to be assessed. If the Drafting Team does not believe this list is complete or appropriate, a complete list of factors should be provided. Without clear guidance, as to factors that should be considered, there is substantial compliance risk if a subjective auditor disagrees with the risk factors identified by an entity

R 1.1.1 – The use of the term “deployment” can be read to require an ongoing obligation even after the software or hardware is in production (i.e. once deployed). To avoid confusion, the term “deployment” should be removed or clarified.

4) For R1: This requirement requires both the development and the implementation of a plan. Recommend breaking this into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement plan in future contracts.

5) For R1: We recommend stating the responsible entity is not required to renegotiate or abrogate existing contracts. The rationale from R1 states that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.” This should be incorporated into the Requirement itself.

6) For R1.1 and the R1 Rationale: The R1 Rationale and the Guidance document list "planning, acquisition and deployment" and versions of these terms in the diagram. R1.1 uses "planning and development". The meaning of "development" has not been clarified and is not part of the process addressed by this standard. Suggest that "development" be clarified or removed.

7) For R1.1.2: We seek further clarification of the intent. As, written the requirement is ambiguous:

a. Is the intent to have the entity evaluate potential methods to mitigate risk? or;

b. To evaluate the effectiveness of mitigating that risk? or;

c. Is it meant to identify the controls in place to mitigate the identified risks?

8) For R1.2.1: The words "Security Event" are in quotes the first time that they are used in the Guidelines and Examples document (page 6). If the Guidelines and Examples document is providing a definition to be applied here, then" Security Event" should be replaced or clarified in the Requirement. This clarification could include "any identified, threatened, attempted or successful breach of the vendor's components, software or systems used in the support of the Entity's BES Cyber System." This new language differentiates R1.2.1 from the vulnerabilities in R1.2.3

9) For R1.2.1: Page 6 of the Guidance and Examples document list both notification from the vendor and notifications from the entity. The R1.2.1 language is unclear in requiring both notifications. Request an update to the Guidance and Examples or the Requirement, for consistency.

10) For R1.2.2: The requirement for the" process for notification" is very different than the "request vendor cooperation" guidance given on page 6, line 22 of the guidance document the requirement as written would require that a process be defined and implemented. The failure of a vendor to notify the entity would, at a minimum be a violation of the entities process or maybe even a compliance violation as a failure to implement the process. Would like to see an additional statement in the requirement language that "A failure of a vendor to follow a defined process is not a violation of this Requirement."

For R1.2: A newly added (in the 1/19/17 draft) sentence in the Rationale (R1) section states: "Implementation of elements contained in the entity's plan related to Part 1.2 *is accomplished* through the entities procurement and negotiation process. Who determines whether it was a sufficient effort to "implement the elements" as part of the procurement and negotiation process? What if you take their first "no" for an answer – is that sufficient effort to implement? Who gets the final sign off?

11) Request clarification - May a responsible entity's procurement plan identify and mitigate risks without requiring vendor involvement for each identified risk?

The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an *existing contract*? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard.

Requirements overlap with existing CIP standards and create double jeopardy situations. Change 1.2.7 from pointing to 1.1.2 to 1.1.1

The following statements from the R1 Rationale box are important caveats for compliance and should be included in the Requirement text:

“Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts.”

“Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan.”

Likes 0	
Dislikes 0	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	

- What is meant by “if applicable” in the Requirement. If this means EACMS/PACS/PCAs for high and medium impact BES Cyber Systems, then state this.

• Extending the applicability to all BES Cyber Systems and associated EACMS/PACS/PCAs results in an unfathomable expansion in scope. For example, in a small Medium Impact Control Center BES Cyber System, we have between 50 and 60 individual software and hardware contracts to manage. Most common industry practices would base the procurement policies for these contracts based on their financial risk, or contracts above a certain spending threshold. However, managing cyber risk does not relate to spending. A million-dollar EMS system could carry less cyber security risk than a $20 camera or a one thousand-dollar network switch. This implies a centralized procurement office for all purchases, since each potential purchase needs to be evaluated for the Cyber Security risk it presents. This would have tremendous costs for smaller entities. We suggest limiting the scope to high and medium impact BES Cyber Systems. • 1.2.3 should read “known [security] vulnerabilities”. Vulnerabilities include any weakness in the code. • What does coordination mean in 1.2.4 and 1.2.6? • Remove 1.2.7. This does not belong in a mandatory and enforceable Standard. As it stands, an entity is required to add other indeterminate processes.	
Likes 0	
Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	

Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
R1.1 is acceptable in regard to entities having a plan to identify and assess risks with procured equipment. R1.2 is unacceptable because the entity creation of Detective Controls for the four Objectives of P. 45 is considered out of the Entity's scope. If only one Entity and one Vendor existed, the individual sub-parts of R1.2 would be feasible for a control plan – but this approach is not viable for hundreds of Entities and dozens of vendors. The Entity is capable of identifying Preventative Controls, in concept, but they will only be effective if the vendors in the supply chain make a diligent effort to implement the controls to the first-line suppliers. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified. Corrective Action Controls are critical, but would be able to be implemented only after a problem is identified.	
Likes 0	
Dislikes 0	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	

FERC didn't specifically ask for Low Impact BES Cyber Systems to be included but didn't explicitly exclude them either. SunPower does not believe Low Impact Cyber Systems should have to meet the same expectations of High and Medium Impact Cyber Systems. While we appreciate the efforts of the SDT to meet the expectations of the FERC Order, we believe the SDT may have gone beyond what FERC was asking them to do.

CIP-003-6 does not require Entities with Low Impact Cyber Systems to have to list the BES Cyber Systems, with this new requirement, do Entities lose their exception? If there is an expectation of that Low Impact Cyber System Entities must adhere to the same or lesser requirements as High and Medium Impact Cyber System Entities, then perhaps CIP-003 would be a better place for the exception. SunPower believes CIP-013, as written, is in direct conflict with the intent of CIP-003-6.

Likes 0	
Dislikes 0	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	

Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 1. In addition, we offer the following comments:

Remove Identify, Assess, and Control Found at the Requirement Level We suggest deletion of these words and terms. The use of identify, assess, and control (IAC) is represented by the responsible entity's governance and control structure. This is an evaluation performed by the Regional Entity in evaluation of the responsible entity's inherent risk and oversight model.	
Likes 0	
Dislikes 0	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
Oxy disagrees that R1 should be applicable to low impact BES Cyber Systems. Although FERC is silent on whether low impact should be included, Paragraph 2 of Order No. 829 says "nor does the Commission require NERC to propose "one-size-fits-all" requirements. The new or modified Reliability Standard 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." The language of R1 elevates low impact BES Cyber Systems to the level of medium and high impact BES Cyber Systems. For example, R 1.2.2 requires a process for when vendor employee remote or onsite access should no longer be granted. Under existing CIP Standards, Access Management Program requirements reside in CIP-004 and none are applicable to low impact BES Cyber Systems. R 1.2.5 requires processes for verifying software integrity and authenticity of all software and patches that are intended for use. Under existing CIP Standards, Security Patch Management requirements reside in CIP-007 and none are applicable to low impact BES Cyber Systems. Additionally, software and patching typically occurs at the Cyber Asset level and low impact entities are only required to identify assets containing low impact BES Cyber Systems. As currently written, R1 and its sub-requirements seem to require an inventory of Cyber Assets or BES Cyber Systems, neither of which are required of low impact entities, which is another element that elevates low's to that of medium and high. Using a risk based approach, it seems more appropriate that R1 be applicable to medium impact and high impact only. The risk assessments are required and performed under CIP-002 and the determination made that low impact BES Cyber Systems pose	

a minimal threat to the BES. Finally, under the existing CIP suite of standards, requirements applicable to low impact entities reside in CIP-003. If a risk management plan is to be required, low impact with a reduced set of requirements to address their minimal BES risk, Oxy requests that those requirements be included as an element of R5 so all the low impact requirements are together or, ideally, included in CIP-003 along with the content of R5. Oxy also requests that CIP-013-1, R1 be rewritten to be applicable to medium and high impact BES Cyber Systems only.	
Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

- Regarding R1.2.1, vendors will unlikely to share security events. Registered Entities should not be held accountable for compliance obligations in which they have no control of.
- Regarding R1.2.1, the Standard Drafting Team should clarify what is intended by, “vendor security event.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.3, the Standard Drafting Team should clarify what is intended by, “known vulnerabilities.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.4, the Standard Drafting Team should clarify what is intended by, “cyber security incidents.” This is an ambiguous term which can have different meanings.
- Regarding R1.2.4, vendors will be unlikely to share cyber security incidents. Registered Entities should not be held accountable for compliance obligations in which they have no control of.

• Regarding R1.2.5, this requirement is duplicative of CIP-007-6. The Standard Drafting Team should clarify how proposed requirement would be completed within the Procurement phase. • Regarding R1.2.6, this Requirement is duplicative of CIP-005-5. .	
Likes 0	
Dislikes 0	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
The scope of the requirement is not clear due to the phrase "if applicable." Please clarify how an entity would determine if their Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets are applicable. Due to some vendors offering many of their products and services outside of the electric utility industry (Microsoft, Cisco, Symantec, GE…) there is a concern that entities will lack leverage when negotiating these new terms and will likely find it difficult to come to an agreement. There are also instances where there are very few options available to industry for a particular product, device, or service. Does the SDT envision that registered entities would be forced to find alternative vendors or products if they are unable to come to an agreement? It is not clear if the requirements are only applicable to new software purchases or also apply to upgrades of existing software (including adding additional licenses for existing software) or renewals of software maintenance contracts that provide software upgrades of existing software. If the existing software is already in place, there is concern that there will be the lack of leverage to require vendors of existing software to negotiate new terms.	
Likes 0	

Dislikes 0	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
SVP agrees with other entity comments to limit this requirement to High and Medium only, as current low impact requirements does not require entities to conduct an inventory of equipment and software or identify systems. Pleas also see APPA's comments, with which SVP is in agreement.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	

Answer	No
Document Name	
Comment	

The need for such a broad set of requirements is unnecessary due to the existing CIP requirements for the entity to have an incident response plan, anti-virus protection and patch management. To the extent the following items remain in R1, NRECA proposes the following actions:

R1.2 – Recommend deleting text after "BES Cyber Systems" as the text is unnecessary.

R1.1.1 – Clarify what is meant by "vendor security events."

R1.2.3 – What is the basis for determining what are "known vulnerabilities?"

R1.2.4 – Clarify the scope of this language as it seems unnecessarily open-ended.

R1.2.5 – Clarify that this item is for BES Cyber Systems only.

R1.2.7 – Delete as it is unclear and unnecessarily open-ended.

Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns:

The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that "address process(es)," and yet, the contents of the requirements include "verifying software integrity." Responsible Entities are familiar with various existing CIP requirements that mandate the development of "processes," but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns:

The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that "address process(es)," and yet, the contents of the requirements include "verifying software integrity." Responsible Entities are familiar with various existing CIP requirements that mandate the development of "processes," but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor's software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor's software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.

Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	

The applicability of this requirement should be limited to high and medium impact BES Cyber Systems. Low impact Cyber Systems are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES. We can re-evaluate at a later date whether additional requirements should be established for low impact BES Cyber Systems.

Using "if applicable" adds confusion to the language. If it is not always applicable to associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets, define where it is applicable and where it is not.

We're concerned that the word "Evaluate" in requirement 1.1.2 might imply that all possible methods for addressing the risks will need to be evaluated. We prefer replacing the term "Evaluate" with "Identify". Additionally, there may be occasion where a risk is identified but is judged to be at an acceptable level given the ability or inability to address it. This standard, in its entirety, should be about minimizing the risks and/or providing reasonable assurance which may result in some instances where the entity will accept a certain level of risk as reasonable. Therefore, we propose the following language: 1.1.2. Identify methods to address the above risk(s), as needed.

Requirement 1.2.1 requires "Process(es) for notification of vendor security events". CIP-007-6 R4 Security Event Monitoring includes a requirement for generating alerts for security events. Assuming that Requirement R1.2.1. is intended to mean the entity will have a process to encourage and direct vendor notification to the client, we suggest this be included in the language of CIP-007.

Requirement 1.2.2 requires "Process(es) for notification when vendor employee remote or onsite access should no longer be granted" The revocation of access, including Interactive Remote Access is currently addressed in CIP-004-6 R5. If this is attempting to require something above and beyond those requirements, it should be made clear what that is and consideration given to housing all of these requirements in CIP-004.

Requirement 1.2.3 requires "Process(es) for disclosure of known vulnerabilities". Is this asking for entities to have a process for the entity to disclose vulnerabilities? Who would we be disclosing to? If it's directed at vendors, the entity can discuss this with the vendor, but the vendor is under no obligation to disclose vulnerabilities and neither the entity, nor FERC, has the authority to require this. Vendors MAY disclose vulnerabilities, but that will likely occur concurrent with providing a fix/patch.

Requirement 1.2.4 requires a "Coordination of response to vendor-related cyber security incidents". From our understanding of what this requires, we believe this is already covered in the entities cyber security incident response plan (CIP-008).

Requirement 1.2.7 requires “Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable”. While we understand what this requirement is intending to do, we believe it is may lead to second-guessing by auditors and/or unrealistic auditor expectations.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements; however, EPE would like to emphasis one issue that is at the forefront of its concerns:

The proposed language of the requirements (especially Requirement 1.2) speaks in terms of using controls that “address process(es),” and yet, the contents of the requirements include “verifying software integrity.” Responsible Entities are familiar with various existing CIP requirements that mandate the development of “processes,” but in CIP-013-1, the inclusion of responsibility for verifying software integrity places a Responsible Entity in a conundrum not present in the other Reliability Standards. Must a Responsible Entity start hiring employees with software capabilities equal or better than the software developers on the staff of the vendors who have historically supplied software products to the industry? If so, how long will that take and at what cost to ratepayers, and can a third party effectively or efficiently create a pool of talent superior to the actual developers of the vendor’s software itself?

Perhaps there is room in the standard for a Responsible Entity to simply require in its processes that any vendor will provide an attestation to the Responsible Entity that the vendor’s software product is authentic and has integrity for the intended use, making this type of attestation a means of complying with the verification requirements found throughout CIP-013-1 in its proposed form. If so, the current wording of the draft standard does not plainly or clearly say so.

EPE understands the objective of the standard, and the Commission's desire to tackle the risks that stem from third party vendors whose work may impact the BES. Our participation in the balloting process for this standard is with the goal of arriving at language that is clear and that enables a Responsible Entity to comply.	
Likes 0	
Dislikes 0	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	Final_Unofficial_Comment_Form_2016-03_03162017_ERCOT comments.docx
Comment	

ERCOT supports the IRC comments and offers the following supplemental comments.

FERC Order 829, Paragraph 59, states that NERC's new or modified 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." This does not include the Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) listed in R1. These systems do not perform or provide bulk electric system operations. ERCOT believes the inclusion of these systems in the draft standard goes beyond the scope of the standard intended by FERC and recommends the SDT remove them from the applicable systems of the standard language.

Requirement R1 requires Responsible Entities to have a plan that addresses processes for notification of a vendor's cyber security events (R1.2.1) and vulnerabilities (R1.2.3), as well as coordination of cyber security incident response activities (R1.2.4). As this information is highly sensitive, it is unlikely that all vendors will agree in all cases to provide this information unless they are already required to do so under other regulatory obligations. Responsible Entities cannot force a vendor to agree to these terms, and in cases where the vendor deems the risk of this disclosure too great compared to the value of the contract, the vendor will decline to enter into the agreement. This will force the Responsible Entity to seek another vendor that is willing to accept these terms, and such a vendor may or may not exist. Because it is possible that a Responsible Entity may be unable to identify a vendor that is willing to accept a contract with the terms required by R1, the proposed standard could seriously hamper the essential functions of Responsible Entities. To address the concern, the drafting team should

include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R1. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)

Requirement R1.2.2 requires "notification when vendor employee remote or onsite access should no longer be granted." The revocation of access, including Interactive Remote Access, is currently addressed in CIP-004, R5. Since the background checks, training, access authorization, and access revocation for employees and vendors is already addressed in CIP-004, the drafting team should ensure any new requirements related to access revocation of vendors be placed in CIP-004. In developing the CIP Version 5 standards, extensive work was undertaken to ensure that all requirements related to the subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework.

Requirement R1.2.5, which requires a Responsible Entity's plan to include "Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use," is duplicative of Requirements R3 and R5 within this standard, which also require documentation of processes. ERCOT recommends removing R1.2.5.

Requirement R1.2.6 requires an entity's plan to include "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)." This requirement is duplicative of Requirement 4 within this standard. ERCOT recommends removing Requirement R1.2.6, which also requires documentation of processes.

Likes 0	
Dislikes 0	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	
Comment	
Requirement R1 states “supply chain risk management plan(s)” while M1, R2, M2 states “supply chain cyber security risk management plan(s)”. ReliabilityFirst recommends the SDT use consistent language so that there is no confusion on terminology.	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes

Document Name	
Comment	

While in overall agreement with Requirement 1, ACEC does have the following concerns:

1. Part 1.1 requires the Responsible Entity to identify and assess risk(s) and evaluate methods to address identified risks. This requirement specifically changes the methodology for risk assessment defined in CIP-002-5.1. As noted in the Background section (Section 6) of the standard, "This general process of categorization of BES Cyber Systems based on impact on the reliable operation of the BES is consistent with risk management approaches for the purpose of application of cyber security requirements in the remainder of the Version 5 CIP Cyber Security Standards." This view of risk based upon the impact of BES Cyber Assets based upon the impact to the BES, not the devices cyber security risk, was defended by NERC and approved by FERC in Order 791 approving Version 5 of the CIP Standards. Based upon this, it would be consistent with CIP-002-5.1 to remove Part 1.1 of Requirement 1, modify requirement R1, Part 1.2.7 to state "other process(es) to address risk(s) as determined in CIP-002-5.1 R1, Parts 1.1 and 1.2" and to add to requirement R1 that it only applies to high and medium impact BES Cyber Systems as used in R3 and R4.

2. In the Rationale for Requirement R1, the term vendor is defined as "(i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators." ACEC is concerned that by including product resellers or vendors, who have no direct or indirect control of these areas, misapplication of the procurement language in this Standard would impose unrealistic obligations, standards of care, and potential liability on professional services related to the supply chain. As a consequence, services currently provided by engineering firms may be uninsurable under current professional liability insurance policies. Other industries supporting the supply chain have raised similar concerns, noting that the effect of this approach will be to stifle competition, impair innovation, and increase costs.

Specifically, the guidance language in this Standard includes "integrator" requirements that impose responsibilities on engineering firms and other supply chain elements for control of software development; personnel management systems; industrial system controls (SCADA); and long- term or post-contract reporting/remediation requirements (vulnerability testing and mitigation). Engineering firms do not typically develop such software and hardware, yet the guidance language suggests they should assume such liability for their use. They also do not monitor and report vulnerabilities for vendor software and hardware. This "one-size-fits-all" approach amounts to a significant reallocation of risk, imposing liability on engineering firms that they can neither manage, nor price. The result will be fewer firms willing to perform

services for this industry. This requirement should be modified to limit the scope and responsibilities to the vendor and end user to ensure risk is apportioned to the responsible parties.	
Likes 0	
Dislikes 0	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

Requirement R1 requires a documented 'supply chain risk management plan', AZPS requests clarification and renaming of the plan to 'vendor risk management plan' throughout the Standard as this term more appropriately describes the content that is required to be included in the plan. Also, the statement …'the plan(s) shall address:' seems redundant and potentially creates a distinction that is not intended. AZPS recommends striking the last sentence and appending …'including' to the first sentence of Requirement R1. Finally, AZPS recommends revising the language of Requirement R1 to focus on BES Cyber Systems and to allow the plan content to address when the associated "Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets" are brought into the scope of such plans as follows:

R1. Each Responsible Entity shall implement one or more documented ***Vendor*** risk management plan(s) that address controls for mitigating cyber security risks to BES Cyber Systems, ***including***: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. The use of controls in BES Cyber System planning and development to:

1.1.1. Identify and assess risk(s) during the procurement and deployment of vendor products and services; and

1.1.2. Evaluate methods to address identified risk(s).

1.2. The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems:

1.2.1. Process(es) for notification of vendor security events;

1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3. Process(es) for disclosure of known vulnerabilities;

1.2.4. Coordination of response to vendor-related cyber security incidents;

1.2.5. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

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

1.2.7. Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.

1.3. The applicability of controls to associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

AZPS also requests that two (2) definitions utilized in the Technical Guidance and Examples be proposed for inclusion as defined terms in the standard, “Security Events” and “Vendor.” Specifically, AZPS notes that Requirement R1.2.1 uses the term “security events” as an undefined term in the Standard, but that the Technical Guidance and Examples, Page 6, uses “Security Events” as a defined term. AZPS requests consistency between the two documents and the addition of the defined term “Security Events” to the Standard. Additionally, AZPS requests the removal of ‘identified, threatened, attempted’ from the defined term and require only notification of ‘successful breach of vendor’s components, software or systems that have potential adverse impacts to the availability or reliability of BES Cyber Systems’. Further, the Rationale for Requirement R1 defines the term “vendors” as ‘(i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators’, AZPS requests incorporating this definition in the Standard for specificity of scope.

AZPS requests clarification regarding the term “processes” as used in Requirement R1.2. In particular, AZPS requests clarification that these items or “processes” are to be included in the overall plan and do not require a separate process or process documentation. Finally, the

Rationale for Requirement R1 states that “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement the Entity’s plan;” however the Requirement does not make clear that the failure of contract negotiations to result in specific controls would not be considered a failure to implement.	
Likes 0	
Dislikes 0	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	

PSEG agrees with the intent of this requirement, but has the following questions/recommendations below:

- The term vendors as used in the standards is defined in the Rationale for Requirement R1 box. This term should be officially defined in the Glossary of Terms used in NERC Reliability Standards.

- Is requirement R1 applicable to new additions and/or modifications to existing BES Cyber Systems? There is not sufficient information to determine if this requirement is applicable only to new BES Cyber Systems or if it also includes changes to existing BES Cyber Systems.

- The applicability of Requirement R1 to High/Medium/Low BES Cyber systems and EACMs, PACs and PCAs is not clear the way it is written. Recommend using the applicability tables as in CIP-004 through CIP-011 for the requirements in this standard, especially R1.

- Requirements 1.2.1 through 1.2.6 discuss processes for vendor controls but some of the controls are unclear as to who is expected to perform the “notification”. For each sub-requirement, PSEG recommends adding clarity in the requirement language indicating who is expected to perform the notification, the vendor or the registered entity.

• Requirement 1.2.1 discusses a vendor security event. This is a vague term. The standard should include more clarification on what a vendor security event is or define the term.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company strongly encourages the SDT to consider the below edits, which use phrasing directly from the FERC Order. If R1 is intended to address the true supply chain procurement side of things, then the proposed edits provided below appropriately scope this requirement at the 'main R' level. The Order 829 Summary, and paragraphs 10 and 24 of the Order specify controls for vendors that supply "industrial control systems" products and services. Therefore, R1 should be focused on to what vendors and what software/firmware this requirement should be limited. The expansion of scope at this stage to propose including all impact classifications of BES Cyber Systems and their associated EACMS, PACS, and PCAs is above and beyond the Order, in our opinion. It's absolutely unmanageable if not restricted somehow to higher level systems. In CIP audits, "BES Cyber Systems" immediately turn into a list of hundreds or thousands of "programmable electronic devices."

The proposed edits provided below move the "planning and procurement" phases of the lifecycle up from sub-requirements 1.1 and 1.1.1 to the main requirement so that all of the sub-requirements under R1 are appropriately scoped as well. Without this, for example, R1.2 applies to all risks at all times throughout the entire lifecycle of all devices. It's cleaner to have the 'main R' be about the plan and setting the scope of the plan, and then have the sub-requirements address the plan(s) specifics. Consistent with Order 829, language from the rationale section addressing the "forward-looking" nature of this new requirement(s) has been incorporated into the main R1 requirement itself. Modifications highlighted below in R1.2.5 are recommended to eliminate redundancy and avoid confusion, while also addressing the specifics in the Order for dealing with "cyber incidents." The order of the sub-requirements of R1.2 have also been adjusted to more clearly align with the planning and procurement life-cycle, while at the same time continuing to address directives in the Order.

Additionally, Southern Company agrees with comments submitted by Georgia Transmission Corporation (GTC), specifically with regard to defining the term "Supply Chain" in accordance with the Order-referenced NIST 800-53 defined term which establishes the applicable time horizon for this Standard, and removal of references to Electronic Access Control and Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.

Modify the R1 language as follows:

R1. Each Responsible Entity shall implement one or more documented supply chain risk management plan(s) that address controls for mitigating planning and procurement cyber security risks for industrial control system vendor products and services used in BES Cyber Systems. Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts. The plan(s) shall address: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 Process(es) for the identification and assessment of risk(s) *of industrial control system vendor products and services*.

1.2 Methods to evaluate controls to address identified risk(s) in R1.1, that includes the following:

1.2.1 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s);

1.2.2 Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3 Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;

1.2.4 Process(es) for disclosure of known vulnerabilities in vendor products;

1.2.5 Process(es) for notification of and coordination of response to vendor-related cyber security incidents; and

1.2.6 Other process(es) to address risk(s) as determined in Part 1.1, if applicable.

Likes 0	
Dislikes 0	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Jeanie Doty - Austin Energy - 5	
Answer	
Document Name	
Comment	
For all Questions - I support the comments of Andrew Gallo, Austin Energy	
Likes 0	
Dislikes 0	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	

Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	

The draft Requirement R1.2 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R1.2, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless a vendor agrees to notify the Responsible Entity of vendor-identified vulnerabilities in the Cyber Assets provided or maintained by the vendor, Responsible Entities cannot comply with R1.2.3.

Responsible Entities could encounter scenarios where:

• Vendors may refuse to comply with the Responsible Entity's vendor controls;

• Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;

• Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or

• Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's required controls. Such a "safety valve" would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Guidance language in the G&TB portion of a Standard is helpful, but the "safety valve" concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary “safety valve” along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.	
Likes 0	
Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	

2. The SDT developed CIP-013-1 Requirement R2 to address the Order No. 829 directive for entities to periodically reassess selected controls and keep plans up to date with emerging cyber security supply chain risk management concerns and vulnerabilities (P 46). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Summary Consideration. The SDT thanks all commenters. The SDT has revised the requirement to review supply chain cyber security risk management plans in response to stakeholder comments. The revised requirement is Requirement R3 in the second draft of CIP-013-1.

Specific comments and SDT responses are provided below:

Commenters recommended that the SDT clarify guidance that Responsible Entities must consider in periodic reviews; some commenters suggested removing Parts 2.1 and 2.2 because they were addressed in the main requirement. The SDT clarified requirements for Responsible Entities to review supply chain cyber security risk management plans every 15 months and removed administrative or ambiguous parts. Rationale section was reworded to indicate that the list of sources of information for reviews is an example for consideration by the Responsible Entity. Implementation Guidance provides an example of a way that a Responsible Entity could be compliant with the requirement.

Commenters recommended clarifying when Responsible Entities were required to obtain initial approval of supply chain cyber security risk management plans. The SDT has added initial approval to the Implementation Plan.

Commenters asked what the impact of implementation would be on contracts that were in development. The SDT intends for implementation to affect contracts that are initiated after the effective date of the standard. Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. The SDT added this information to the Implementation Plan.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	

Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The Rational for Requirement R2 lists several sources for supply chain vulnerabilities, but it is not clear what is considered a relevant source and whether the entity is required to review all sources of supply chain vulnerabilities which may be very burdensome. CenterPoint Energy recommends adding the specific sources of vulnerability information, such as E-ISAC or ICS-CERT in the requirement.	
Likes 0	
Dislikes 0	
Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	

1) Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2. 2) For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans. 3) Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.	
Likes 0	
Dislikes 0	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
David Rivera - New York Power Authority - 3	
Answer	No
Document Name	

Comment
1. Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2. 2. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans. 3. Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months. 4. SDT should clarify that existing contracts do not need to be renegotiated based on the 15-calendar month reassessment of the plan or other plan revisions. 5. Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

NRG recommends that each requirement should have a provision for allows an entity to accept the risk of selection a vendor that will not or cannot supply a control. NRG recommends removal of R2.1 language which is covered in R2.

For R2, will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? This seems to imply scope creep from elements on R1. Is "necessity" defined by entity, NERC, or outside source?

NRG requests clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Dominion recommends that requirement R2 be replaced with the following:

"Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 related to procuring and installing unsecure equipment or software, the risk of unintentionally failing to anticipate security issues that may arise due to network architecture, unintentionally arise during technology and vendor transitions, and purchasing software that is counterfeit or that has been modified by an unauthorized party at least once every 15 calendar months, which shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*"

Dominion is of the opinion that the activities specified in Part 2.1 are included in the language of R2. Dominion recommends modifying Part 2.1 and 2.2 as follows:

- 2.1 Revision(s), if any, to address applicable new supply chain security risks that include security considerations related to cyber security, and
- 2.2 The supply chain plan(s) shall be reviewed, updated as necessary, and approved by CIP SM or delegate at least once every fifteen (15) months.

Also see the recommendation for replacing this requirement as described in the comments for R1.

Likes 0	
Dislikes 0	

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment

Refer to our comments on R1.

We do not agree with the approach in R1 (and R2) of creating “plans” and the intent of the plans to “cover the procurement aspects of all four objectives.”

Order 829’s four objectives did not include creating “plans.” All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011.

NERC’s Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets.

With respect to R2 as proposed, 1,398 entities would have to annually research information, including information which is readily available to be proactively provided by NERC to them. This diverts and dilutes registered entities' resources.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

Exelon feels that the R2.1 language is vague and has the potential to become administratively burdensome without a corresponding benefit to BES reliability. While Exelon agrees with the rationale that examples of sources of information that an entity could consider include guidance or information issued by the E-ISAC, this language should be included in the Requirement itself because only that language forms the basis of a compliance assessment. Exelon receives over 100 security-related messages regarding potential vulnerabilities per day from a myriad of sources. Without creating bounds around the sources to be considered as well as the periodicity for updates to supply chain cyber security risk management plan(s), the question of whether any or all of the messages should have been considered will be difficult, if not impossible, to evidence. Exelon points out that the E-ISAC already performs important filtering functions for the industry. Perhaps future Alerts issued by the E-ISAC could be enhanced to point out vulnerabilities that would require new mitigating controls in supply chain cyber security risk management plan(s). Without these limitations, each entity will need to develop processes and procedures to receive and filter information, define mitigating controls, update the plan(s) and obtain approvals which is inefficient at best and impossible to evidence at worst.

Further, Exelon suggests that while multiple updates to the plan(s) may occur within a year as new E-ISAC Alerts are issued, CIP Senior Manager Review and Approval should only be required every 15 months. Intermediate reviews and approvals, or reviews for minor changes, should be outside the scope of the Requirement.

Likes 0	
Dislikes 0	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
We suggest moving this Requirement language to the CIP-003 Standard. Our group feels that CIP-003 is the most appropriate Standard to handle this Requirement which is applicable to Low Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Approval of CIP Senior Manager or delegate should be required for both or neither of R1 and R2.	
Likes 0	
Dislikes 0	
William Harris - Foundation for Resilient Societies - 8	

Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See comments on Requirement R2 in attached file.	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	
Comment	
Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013.	

The language of R2.1 appears redundant and not any different than what is already required in the language of the main requirement, R2. Suggest deleting R2.1.	
Likes 0	
Dislikes 0	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Please refer to RSC- NPCC comments	
Likes 0	
Dislikes 0	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	
• As previously stated, for consistency with other CIP Standards (e.g. Physical Security plans, Incident Plan, Recovery Plans, Information Protection program, etc..) , CIP-003 R1.1 should be expanded to include the Supply Chain Risk Management plan as part of the collective cyber security policies reviewed and approved by the CIP Sr. Manager at least every 15 months. And, applicability of supply chain risk management controls to assets that contain Low Impact BCS should be consigned to CIP-003, R1.2 and R2. • The NERC Glossary of Terms definition of CIP Senior Manager will require update to include CIP-013	
Likes 0	
Dislikes 0	
Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	No
Document Name	
Comment	
R2 contains the language “As necessary… at least once every 15 months…” Is it an “as necessary” requirement or is it once per 15 months? Recommend removing the “as necessary” language as it is too subjective and open to interpretation.	
Likes 0	
Dislikes 0	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

1. Suggest deleting R2.1. The R2 language includes “review and update as necessary”. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

2. For R2.2: Page 9 of the Guidance and Examples document states “Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review.” CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

3. Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

Likes 0	
Dislikes 0	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	

Comment
AECI supports the following comment from AEP: "R2 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R2 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R2 should be rewritten to be only applicable to high and medium impact BES Cyber Systems."

Likes 0	
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	

Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
R2 has no stated applicability and it is unclear whether the CIP Senior Manager approval required here is any different from the required approval under R5. It would be clearer if R2 were made into R1.3, with the clarification suggested in our comments above to clearly exclude Low BES Cyber Assets from this requirement and consolidate requirements for those assets under R5.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
What is the target of the word “revisions” at the beginning of R2.1? Does revisions refer to modifications of the “supply chain cyber security risk management plan(s)” document itself? If so, then requirement is redundant in that R2, and consequently R2.1 could be interpreted to	

require entities to evaluate the revisions that were just completed. Or is the intent of “revisions” to direct REs to consult document(s) external to the standard when executing revisions?	
Likes 0	
Dislikes 0	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Strike R2.1 because the R2 language includes “review and update as necessary” covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.	
Likes 0	
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
R2 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R2 be rewritten to address	

the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R2 should be be rewritten to be only applicable to high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John
Dislikes 0	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	

Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No

Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
R2 – first line – for clarity purposes NRECA recommends removing “and update, as necessary.” R2.1 – strongly recommend deleting “to address applicable new supply chain security risks and mitigation measures” as it is unclear and unnecessarily open-ended.	
Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	

SVP agrees with other entity comments that "additional evaluation of the revisions is an administrative task that does not enhance BES security."	
Likes 0	
Dislikes 0	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months and removed from CIP-013-1.	
Likes 0	

Dislikes 0	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 2.	
Likes 0	
Dislikes 0	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
The way the Requirement is written once again leaves the Requirement open to interpretation. The current text reads: "Each Responsible Entity shall review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, which shall include:" SunPower believes the correct statement of R2 should read:	

"Each Responsible Entity shall review, as necessary, but at least once every 15 calendar months, its supply chain cyber security risk management plan(s) specified in Requirement R1 and update as necessary. The reviews and updates includes, but not limited to:" SunPower also believes that the intent of R2.1 is not clear when the Requirement states, "to address applicable new . . . " SunPower believes the term "applicable" needs to be left out of the Requirement unless the SDT is talking to the Applicability Section of the Standard, if that is the case, then state the Applicability Section. If that is not the case, SunPower believes the sub part should read: "2.1 Evaluation of revisions, if any to address newly identified supply chain security risks and mitigation measures"	
Likes 0	
Dislikes 0	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	

Agree that it is appropriate to reassess the Entity plan associated with R1.1, but updates to the R1.2 portion would be unmanageable to point of being non-productive for entities and suppliers, for the reasons already stated in the R1 response above.	
Likes 0	
Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
The annual assessment of new risk is too open ended for a mandatory and enforceable Standard.	
Likes 0	
Dislikes 0	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) Strike R2.1 because the R2 language includes "review and update as necessary" covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

2) For R2.2: Page 9 of the Guidance and Examples document states "Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review." CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

3) Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

SDT should clarify that existing contracts do not need to be renegotiated based on the 15-calendar month reassessment of the plan or other plan revisions.

Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No

Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
It is not clear if the approval by the CIP Senior Manager is required with the first version of the plans, or only for subsequent revisions. It is not clear if the approval by the CIP Senior Manager or delegate is required with each review cycle or only if modifications are made to the document(s).	
Likes 0	
Dislikes 0	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	

See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
Agree that it is appropriate to reassess the Entity plan associated with R1.1. For the reasons already stated in the R1 response, updates to the R1.2 requirements would be unmanageable to point of being non-productive for entities and suppliers.	
Likes 0	
Dislikes 0	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC knows of no definitive source to identify “new supply chain security risks and mitigation measures.” Therefore, compliance with this requirement part becomes subjective thus is not auditable. Reviewing and updating the plan as necessary under the core R2 along with CIP Senior Manager approval per R2.2 should be sufficient to maintaining a quality cyber security supply chain risk management program. We recommend the removal of requirement part 2.1.	

Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

We feel that there should be some guidance on where to look for "emerging supply chain related concerns". If our company is using a particular source and miss a notification on another site, will we be penalized?

Likes 0	
Dislikes 0	

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	
With regards to the periodic reassessment of supply chain cyber security risk management controls, the IRC and SWG request the SDT provide objective criteria for the scope and content of the review to ensure consistent implementation against set criteria. Does this only require update of the plan document? Do needed contract revisions have to be documented? What is required to demonstrate review and consideration of items that may not be incorporated into the updated plan?	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s). Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.	

We recommend the following language for consideration by the SDT: R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. We feel that there should be some guidance on where to look for “emerging supply chain related concerns”. If our company is using a particular source and miss a notification on another site, will we be penalized? 3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.	
Likes 0	
Dislikes 0	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language. R2 needs a more clear description on when mitigation measures are required. For example, would the selection of one vendor over another be considered a mitigation measure? Would an entity be required to always choose the vendor with the best-in-class security posture despite cost?	
Likes 0	
Dislikes 0	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

The rationale for Requirement R2 suggests that every Responsible Entity should assess all supply chain risks before updating the plan, which may be a very burdensome requirement that will be difficult to comply with and audit. Would a Responsible Entity be in violation if it didn't document that they read a particular DHS report? Also, the Requirement R1 plan is focused on methods to review, assess, and evaluate vendor and vendor product/service risk before entering into a contract with a vendor, these methods are unlikely to change all that much based on guidance issued by NERC or DHS and would be naturally covered by a periodic review and approval of the plan(s).

Also, part 2.1 requires an evaluation of revisions to address new supply chain security risks and mitigation measures. It is unclear how a revision to address a new supply chain security risk is different than a mitigation measure. A mitigation measure addresses a risk.

We recommend the following language for consideration by the SDT:

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	

The NYPA Comments	
Likes 0	
Dislikes 0	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
We believe that sub requirements (2.1 and 2.2) in R2 are unnecessary. Similar verbiage used in CIP-003-6 for review of cyber security policy can be used in this instance. Also, can the CIP Senior Manager delegate this accountability?	
Likes 0	
Dislikes 0	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	

FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
With regards to the periodic reassessment of supply chain cyber security risk management controls, the IESO request the SDT provide objective criteria for the scope and content of the review to ensure consistent implementation against set criteria. Does this only require update of the plan document? Do needed ntract revisions have to be documented? What is required to demonstrate review and consideration of items that may not be incorporated into the updated plan?	

Likes 0	
Dislikes 0	
Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	
This should be removed and convered in CIP-003.	
Likes 0	
Dislikes 0	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
1) Suggest deleting R2.1. The R2 language includes “review and update as necessary”. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.	
Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	No
Document Name	
Comment	
BPA believes if the scope and language for R1 is appropriate, the review process is necessary but should not require CIP Senior Manager Approval. BPA suggests maintaining consistency across standards: CIP Senior Manager approval is required for policies rather than plans.	
Likes 0	
Dislikes 0	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

R2

IPC suggests the SDT consider re-structuring the proposed format for R2 to align with current enforceable standard format (see CIP-002-5.1 R2, R2.1, and R2.2):

The Responsible Entity shall: (1) Review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months, (2) Evaluate revisions, if any, to address applicable new supply chain security risks and mitigation measures; and (Question) How does the SDT foresee this evaluation being measured and accomplished? (3) Obtain its CIP Senior Manager or delegate approval (Question) Is the CIP Senior Manager or delegate intended to be an approval of the plan every 15 months? If so, IPC recommends specifying the timing and what is being approved in the wording of the requirement.

IPC does not believe R2.2 provides any security measures or controls and is simply an administrative exercise. IPC recommends R2.2 be removed.

Likes 0	
Dislikes 0	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016. Reclamation recommends Requirement R2 should instead require entities to implement their supply chain risk management plan(s) developed in Requirement R1. Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.	
Likes 0	
Dislikes 0	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	

1. Requiring a greater level of testing, documentation, or security features from system integrators, suppliers, and external service providers may increase the price of a product or service, and increase the compliance burden for the industry. We recommend language addressing key questions, such as: at what time frame does the risk reduce to acceptable: Daily, weekly, monthly or yearly? How is the standard addressing acceptance of risk?	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	

Likes 0	
Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	

While it is not unreasonable to propose periodic review and reassessment to assure some minimum level of rigor, ultimately Registered Entities know that plans are living documents that must be supported by sound security practices implemented to stay apprised of emerging cybersecurity threats as they enter the landscape, and a 15-month reassessment is ill-equipped to support the pace of the ever-evolving threat landscape. The industry might be better served with language that supports a periodic review coupled with the need for ongoing and timely assessment and update of plans on an as needed basis when the impending threat warrants the action.

The SDT may want to reconsider the need and intended value for CIP Senior Manager approval for these reasons. 1.) While it is not unreasonable to propose an approval for plans of this nature, prescribing this as a CIP Senior Manager responsibility is inconsistent with other enforceable mandatory CIP Cyber Security Reliability Standards that limit these approvals to BES Cyber System populations, policy, and, exceptions (both CIP Exceptional Circumstances and Technical Feasibility Exceptions). 2.) The introduction of CIP Senior Manager or delegate approval may not provide the intended value for the complex range of jurisdictional, technical, economic, and business relationship issues. 3.) By NERC definition, as a technicality, please note that the scope of the CIP Senior Manager accountabilities is currently prescribed as CIP-002 – CIP-011 and would require amendment. 4.) Lastly, as a consideration, the SDT may want to revisit the need for this level of approval and to align the approach with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate requirements are administrative in nature only and therefore that do not provide security or reliability value.

Likes 0	
Dislikes 0	

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	

Dislikes 0	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	Yes
Document Name	
Comment	

1. Strike R2.1 because the R2 language includes "review and update as necessary" covers the FERC Order. Additional evaluation of the revisions is an administrative task that does not enhanced BES security. Make corresponding changes to section M2.

1. For R2.2: Page 9 of the Guidance and Examples document states "Requirement R2 allows responsible entities to incorporate the review of CIP-013-1 into their annual CIP-003 review." CIP-003-6 R1 does not allow delegates to review and approve. In addition, CIP-003 requires the review of Policies and not plans.

Request clarity on how revisions to the plan would need to be addressed for contracts that are in the process of being negotiated since this negotiation process may take months.

SDT should clarify that existing contracts do not need to be renegotiated based on the 15 calendar month reassessment of the plan or other plan revisions.

An entity's plan must be implemented at the commencement of negotiations.

Will NERC, E-ISAC or other sources referenced in Rationale issue annual updates for supply chain risk? How will an entity prove that all risks have been incorporated? Seems to imply scope creep from elements on R1. Is *necessity* in R1 defined by entity, NERC, or outside source?

Likes 0	
Dislikes 0	
Steven Rueckert - Western Electricity Coordinating Council - 10	

Answer	Yes
Document Name	
Comment	
R2 is pretty straightforward, however unless modified by a subsequent implementation plan, WECC would expect an entity to have a reviewed and approved SCRM plan on or before the effective date, then complete R2 on intervals of no more than 15 calendar months. If an entity exceeds the 15 calendar month time frame, an R2 PNC would be indicated.	
Likes 0	
Dislikes 0	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, SRP requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes

Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval. 3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
While supporting this requirement, ACEC recommends that the requirement be modified to state it only applies to high and medium impact, consistent with requirements R3 and R4.	
Likes 0	
Dislikes 0	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	

Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, AE requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
PRPA agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, PRPA requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CHPD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy suggests the drafting team consider collapsing 2.1 and 2.2 into one sub-requirement. We do not see the need in having these as two sub-requirements, and this would mirror the language used in CIP-003-6. Also, the use of the term “applicable” in R2.1, appears vague and could lead to potential disagreement on what supply chain security issues actually pose a substantial risk.	
Likes 0	
Dislikes 0	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Proposed CIP-013-1, R2 properly implements Order No. 829's directive to develop a Standard requiring entities to periodically review and approve the controls adopted to address specific security objectives associated with supply chain risk management.	
Likes 0	
Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	

The use of 15 calendar months allows entities to review and update (as required) on a systematic basis, the same time every year, Thank you.	
Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern Company strongly encourages the SDT to consider the below edits to R2 to make it clear that assessment of risks and revisions to the plan are required on a "once every 15 months" interval, and not at the time of each and every notification of any new potential risks/vulnerability. The below proposed modifications also clarify that *revisions* to the plan(s) are predicated on the existence of "new supply chain cyber security risks" by moving the phrase "if any." Subsequently, R2.2 has been modified to require CIP Senior Manager or delegate approval only when, following a required review every 15 months, it is determined revisions to the plan(s) are warranted to address "new supply chain cyber security risks" or "mitigation measures." As written in the draft Standard, an annual review and approval by the CIP Senior Manager or delegate where no revisions were warranted or made is a documentation exercise that provides no benefit to reliability or reduction of supply chain risk. The SDT should also consider strengthening the language in the Rationale and/or Guidelines directing Entities to adequate and/or designated sources (NERC/DHS/E-ISAC/ICS-CERT) providing Supply Chain guidance for those higher level issues that warrant a change to your plan(s). Also of note and for SDT consideration is the structure of the Implementation Plan for this Standard that does not require the CIP Senior Manager or delegate to review and approve the initial plan(s) on or before the effective date the plan(s) is required to be in place; therefore, review and approval of the plan(s) would be 15 months after the plan(s) was already in effect.

Modify R2 language as follows:

R2. Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in Requirement R1 and update them, as necessary, at least once every 15 calendar months, which shall include:

2.1. Evaluation of revisions to address new supply chain cyber security risks and mitigation measures, if any, related to industrial control system vendor products and services applicable to the Responsible Entity's BES Cyber Cyber Systems; and **2.2.** Obtaining CIP Senior Manager or delegate approval for any revisions to the plan(s).	
Likes 0	
Dislikes 0	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT supports the IRC comments on this question.	
Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Generally, we agree with the requirement to have the CIP Senior Manager review and update, as necessary, its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. However, R2.1 could be interpreted in many ways that might introduce uncertainty in the process. In agreement with EEI, we suggest the following language:	

R2. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval for its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	Yes
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
SMUD agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, SMUD requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management	

plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	
Comment	
Seattle City Light agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Seattle City Light requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	Yes
Document Name	
Comment	

Colorado Springs Utilities (CSU) agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, CSU requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures	
Likes 0	
Dislikes 0	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • Recommend changing Requirement 2.1 from "Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and" to "Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures as determined by the registered entity; and" • The standard language does not address how a revision to the plan needs to be addressed by contracts already in process/negotiation at the time of review or revision. Please provide guidance.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Stephanie Little - APS - Arizona Public Service Co. - 5	

Answer	Yes
Document Name	
Comment	
For consistency and to ensure that the requirement appropriately reflects the scope of risks being addressed, AZPS requests striking of 'supply chain security risks' in Requirement R2.1 and replacing with 'Vendor security risks'.	
Likes 0	
Dislikes 0	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, Santee Cooper requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Ballard Mutters - Orlando Utilities Commission - 3	
Answer	Yes
Document Name	

Comment	
OUC agrees that the plans in Requirement R1 need to be updated and a 15-month review period is appropriate. However, OUC requests the removal of R2.1 and 2.2 and updating R2 to read: Each Responsible Entity shall review its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months, to include reviewing new risks and mitigation measures and identifying related changes, if any, and obtain CIP Senior Manager or delegate(s) approval.	
Likes 0	
Dislikes 0	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Scott Downey - Peak Reliability - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Wesley Maurer - Lower Colorado River Authority - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	

Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Glenn Pressler - CPS Energy - 1	
Answer	
Document Name	
Comment	

CPS Energy supports the comments provided by APPA	
Likes 0	
Dislikes 0	

3. The SDT developed CIP-013-1 Requirement R3 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Summary Consideration. The SDT thanks all commenters. The SDT removed this requirement from CIP-013-1 as recommended by commenters and is addressing the directive by modifying existing CIP standards. The SDT sought input from the Project 2016-02 CIP Revisions SDT and developed Proposed CIP-010-3 Requirement R1 Part 1.6 to address the directive.

Specific comments and SDT responses are provided below:

Commenters stated that the directive should be addressed in other CIP standards. The SDT developed revisions in CIP-010-3 to specifically address directives in Order No. 829 for verifying software integrity and authenticity. The SDT used input from the Project 2016-02 CIP Revisions SDT.

Commenters stated that Responsible Entities need flexibility to account for technical feasibility or vendor capability. In developing the revisions in CIP-010-3, the SDT provided flexibility for meeting the objective *when a method to do so is provided* for the software.

Commenters recommended clarifying or changing the assets in scope for the requirement; or using a table for clarity. The revised requirement in CIP-010-3 is clearly drafted using a table format. The SDT believes the scope of High and Medium BES Cyber Systems is consistent with other configuration change management requirements, and that this will appropriately address the reliability objective for software verification as specified in Order No. 829.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

Suggest “software, firmware, and associated patches” Possible TFE language for R3? The

NSRF recommends the following:

Q 3. Add language to address potential Technical Feasibility Exception (TFE).

R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware**, where technically feasible,** before being placed in operation on high and medium impact BES Cyber Systems:

R3.2

“Firmware” is already included in R3 this redundant in R3.2 recommend R3 to be written as a general Requirement with specifics in the sub Requirements.

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

faranak sarbaz - Los Angeles Department of Water and Power - 1

Answer	No
Document Name	

Comment
The standard as written doesn’t clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.

Likes 0	
Dislikes 0	

Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
TFE opportunity is again needed, especially to address vendor-proprietary (“black box”) vendor software and firmware, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses). R1.2.5 is largely duplicative of R3. They should be made consistent, or one of them should be deleted. R3 may better belong in CIP-007 and needs to be aligned with CIP-010. Requirements for a single topic should be consolidated within a single standard.	
Likes 0	
Dislikes 0	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 3, Williams John

Dislikes 0	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	
It may not be possible to verify the integrity and authenticity of software and firmware before being placed into operation if the Vendor is no longer in business or will not cooperate. There should either be an exception or '*out*' for possibility (e.g. … where possible.), leaving that determination up to an audit team, or a feasibility exception should be allowed.	
Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Change/add language to emphasize that failure to obtain the cyber security controls from a vendor doesn't translate to being out of compliance. Entity should have the ability to mitigate risks posed by vendors. Furthermore, this risk should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-007 R2.	

IID feels that there should be an exclusion or exception (similar to a CIP Exceptional Circumstance or Technical Feasibility Exception) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.	
Likes 0	
Dislikes 0	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Would deployment tools that rely on digital signature enforcement (such as Microsoft Authenticode Security Verification or Red Hat signature verification) satisfy the intent of this requirement where such mechanisms provide technical checks for verification of authenticity and integrity? The requirement measures should allow automated deployment tools such as Microsoft's System Center Configuration Management to be trusted for the purpose of confirming the integrity and authenticity of software and firmware.	
Likes 0	
Dislikes 0	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	

Comment

Duke Energy recommends the following language revision to R3.

"For BES Cyber Systems in production, each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware prior to installation on high and medium impact BES Cyber Systems:"

We suggest the addition of the phrase "For BES Cyber Systems in production," at the outset of the requirement.

We also recommend replacing the phrase "placed in operation" with "prior to installation" in R3. The phrase "placed in operation" is ambiguous, and could be open to debate as to what this actually means. The language "prior to installation" is less ambiguous, the language used in FERC Order 829, and is already used in the rationale section for this requirement.

Also, Duke Energy has some concern with the amount of involvement/cooperation that will be necessary from a vendor in order to achieve compliance with this requirement. Some issues may arise if/when a vendor is not able to verify the integrity or authenticity of a certain product. We suggest the drafting team consider this situation as appropriate for a Technical Feasibility Exception or in some instances be granted a CIP Exceptional Circumstance. For example, an issue could arise wherein an entity has a device that is failing, and a fix (update of software) is needed immediately. In the interest of system stability, there may not be enough time to wait on a vendor to send a certificate of authenticity on a patch or software upgrade. We feel that a Technical Feasibility Exception and CIP Exceptional Circumstance should be considered based on these issues.

Another aspect of R3 that we think requires some clarity is whether or not R3 should apply at the BES Cyber Asset level. Currently, the language explicitly states BES Cyber System, but we feel that the language may not represent the actual intent of the requirement. If the controls proposed in R3 are better suited at the Cyber Asset level, the language should be revised to reflect this.

Lastly, Duke Energy would like to suggest that the drafting team consider that this requirement be moved to current standard CIP-007-6. CIP-007-6 already addresses security controls for BES Cyber Systems, and we feel that this control oriented requirement may be better suited there.

Likes 0	
Dislikes 0	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Requirement R3 mentions high and medium BES Cyber Systems, but does not include their associated Electronic Access Control and Monitoring Systems (EACMs), Physical Access Controls(PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following modifications for consideration:

1. R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems [and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets]:

Likes 0	
Dislikes 0	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	

CIP-007 R2 requires a mitigation plan for patches that cannot be applied within 35 days. Please confirm that if a patch cannot be applied within 35 days due to the vendor's inability to provide the integrity check, there is no other compliance risk if the RE provides a mitigation plan in accordance with CIP-007 R2. Additionally, if vendors refuse or can't provide hashes or other verification methods, please provide confirmation that an internal process to test, scan and perform verification activities would be enough to satisfy this requirement.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	

Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	

Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI urges the SDT to remove R3 and address firmware and software integrity/authenticity in the supply chain risk management plan(s) as detailed in the requirement concepts proposed by AECI in Question 1. This will allow Responsible Entities to address this issue contractually with applicable vendors in the supply chain/procurement process and not the operational time horizon.	
Likes 0	
Dislikes 0	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	
PRPA requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	
AE requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business or will not cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date.

3. The applicability of this requirement should be limited to high and medium impact BES Cyber Systems with external routable connectivity. This would align the standard with the applicability of CIP-007 and CIP-010.

4. Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

5. Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

6. Provide clarity for when a system is pre-loaded by a vendor and delivered to an entity. Is the entity required to verify software authenticity? If a computer is purchased from Dell, can Dell provide authenticity for all of the firm ware that is part of the system but not directly manufactured by Dell; i.e. system bios, sound system, network adapter, video controller.

Likes 0	
Dislikes 0	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	

CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	

I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

This requirement should be incorporated into CIP-007 R2 or CIP-010 R1. This is a System Security Management requirement and belongs in the appropriate location. CIP-013-1 R3.1-R3.4 are all components of the the CIP-010 baseline. Placing this topic in a separate standard and requirement creates compliance confusion. As entities will have to follow different requirements in CIP-007, CIP-010, and CIP-013, there is an increased likelihood of a violation.

As there is no consistency within the software industry on the use of hash functions, there must be guidelines on what is considered an acceptable approach to meet this requirement. While guidelines are needed, it must be understood that many times the individual utility has little influence on software vendors due to the relatively small purchasing power of the electric sector relative to the vendor's overall market.

Likes 0	
Dislikes 0	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No

Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	

- The scope of CIP-013-1 R3 overlaps with parts of CIP-007-6 R2 and CIP-010-2 R1.1-1.5. However, both CIP-007 R2 and CIP-010 R1 apply to High and Medium BCS and associated EACMS, PACs, and PCAs. The potential collision of requirements that apply inconsistently (e.g. BCS vs EACMS) across three standards will be difficult to manage, monitor, and implement. For example, timing of security patch implementation per CIP-007 R2.3 could be impeded by authenticity processes required in CIP-013. Meeting compliance with CIP-013 could unintentionally cause not only potential compliance problems with CIP-007 R2, but also significant security, operational, and/or reliability impacts.

- An exception process is required for R3. This requirement will apply to the existing complement of High and Medium BCS, upon the enforcement date of the new Standard. However, since entities are explicitly not required to renegotiate existing contracts, it may be difficult to meet compliance with this requirement upon enforcement, if existing vendors do not provide appropriate support.

- Measures and Evidence – Since the R3 requires an entity to show that documented processes have been implemented, M1 does not adequately describe the evidence required to demonstrate implementation.

Likes 0	

Dislikes 0	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Please refer to RSC- NPCC comments	
Likes 0	
Dislikes 0	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	

Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	
Comment	

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations.

Does R3 allow the Entity to "accept the risk?"

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request "per system capability" wording for R3. Not all vendors provide a "golden hash" or other mechanism to validate.
- To be consistent with not requiring R1.2.5 we suggest adding the language "subject to procurement contract."

To be consistent with not requiring R1.2.5, we suggest adding the language "subject to procurement contract." There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

Additionally, R3 may hinder an entity's ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where "obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan"

We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
Comments in final section.	
Likes 0	

Dislikes 0	

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment
N&ST strongly supports the goal of verifying software integrity and authenticity and hopes vendors will be generally willing to provide Responsible Entities with checksums, cyber hash values, or other integrity checks for their software and firmware. However, as written the requirement creates the potential for a conflict with CIP-007-6 R2 Part 2.3 (installation of applicable security updates), and could leave a Responsible Entity with potentially no recourse other than to create a mitigation plan if a vendor is for some reason unable or unwilling to provide such integrity verification for a patch or other type of software or firmware update. N&ST recommends that the SDT consider allowing for exceptions that must be (a) fully documented and (b) approved by the Responsible Entity's CIP Senior Manager

Likes 0	
Dislikes 0	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment
We agree with the drafting team that verification to the integrity and authenticity of the software needs to be validated. However, we would ask the question, "If the industry finds validations issues, how do we hold the vendor accountable?" We understand that contracts are in

place to help this situation, but this doesn't always resolve validation issues. We feel that FERC Order 829 language falls short of holding the vendors accountable in reference to addressing verification of software integrity and authenticity and as a result, the compliance burden is placed on the users. The CIP requirements focus on the Responsible Entity carrying the compliance risk even if the industry can identify vendor validation issues. For example, entities could potentially pay for product upgrades to address compliance concerns when it's been verified that the current product upgrades have not met the quality of service that was promised by the vendor. We suggest that the drafting team hold open discussions with FERC, potentially conducting a gap analysis in reference to this potential concern. If the analysis determines a gap, FERC should seek legislation to hold vendors more accountable. Also, we suggest that Requirement R3 language should be moved to the CIP-010 Standard. Our group feels that the CIP-010 Standard adequately addresses software and firmware verification. Additionally, we propose some language revisions to the Requirement language. SPP's proposed language revision to R3: "Each Responsible Entity shall implement one or more documented process for verifying the integrity and authenticity of the following software and firmware before being installed in operation on high and medium impact BES Cyber Systems". The term "installed" has been consistently used throughout the CIP-010 Standard and we feel this will give our proposed language validity and consistency.	
Likes 0	
Dislikes 0	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	
Comment	

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

The draft Requirement R3 language creates compliance concerns due to the need for Responsible Entities to negotiate commercial contracts with vendors that commit the vendors to undertake the tasks necessary for R3 compliance, particularly in circumstances where only a single vendor has the capability of providing the necessary services for Cyber Assets covered by CIP-013-1. For example, unless the vendor agrees to cooperate with any software integrity and authenticity verification process, the Responsible Entity will be unable to ensure the integrity and authenticity of software used in covered Cyber Assets.

Responsible Entities could encounter scenarios where:

• Vendors may refuse to comply with the Responsible Entity's vendor controls;

• Vendors may demand an unreasonably high payment for compliance with the Responsible Entity's vendor controls;

• Vendors may agree to Responsible Entity controls but fail to take the steps necessary to implement those controls in a compliant manner; or

- Software/firmware made by a vendor no longer in business and unable to assist the Responsible Entity in the integrity and authenticity verification process.

To ensure that compliance with CIP-013-1 does not place Responsible Entities in an untenable negotiating position, a compliance "safety valve" is necessary to allow Responsible Entities to comply with the Standard even in the absence of vendor assent to the Responsible Entity's

required controls. Such a “safety valve” would be consistent with the current draft guidance on CIP-013-1 R1.2, which states that “[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan.”

Guidance language in the G&TB portion of a Standard is helpful, but the “safety valve” concept should be included within the language of the Requirement itself because only that language forms the basis of a compliance assessment.

Exelon has sent ideas under separate cover to the Drafting Team Chair outlining three options for providing the necessary “safety valve” along with proposed text edits to the requirements. In short, these options include a technical feasibility exception, a commercial feasibility exception or a simple exception documentation process.

Exelon does not support the draft language in R3 which requires an Entity to verify the integrity and authenticity before placing a BES Cyber System into operation. Instead, Exelon prefers the suggested language from Order No. 829 that directs “the integrity of the software and patches before they are installed in the BES Cyber System environment” (P. 48). Accordingly, Exelon suggests that R3 be edited to read as follows:

Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware **prior to installation into** high and medium impact BES Cyber Systems

Likes 0	
Dislikes 0	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that for future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch.

What does the SDT consider a "secure central software repository"?

Likes 0	
Dislikes 0	

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	

Specific operational cyber security controls are best addressed as revisions to CIP-002 through -011.

Prescribing verification of integrity and authenticity is a “how” not a “what.”

Refer to EEI comments on R3. We agree with the concept of the EEI comments to consider a revision in CIP-010 for a specific security objective (“what”), such as “method(s) to minimize the risk of installing compromised” CIP-010 R1 baseline configuration items.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives’ deadlines, NERC and industry should reprioritize SDT teams’ work and resources.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No

Document Name	
Comment	

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R3 - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into

a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch. What does the SDT consider a "secure central software repository"?	
Likes 0	
Dislikes 0	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	
• Patch Management obligations for cyber security related patches are already addressed in CIP-007. Dominion is of the opinion that the obligations in this requirement would be better placed (once it's determined what the obligations should be) in CIP-010 or CIP-007. • If R3 is kept in CIP-013 and not moved to an existing CIP Standard, we recommend the following: R3: Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following, prior to authorized installation on high and medium impact BES Cyber Systems and associated EACMSs, PCAs, and PACs: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	
Likes 0	
Dislikes 0	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

SCE&G agrees with the concerns and questions raised by the Edison Electric Institute (EEI), including the following:

"Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls. For example, the language could allow a Responsible Entity to use a vendor's website for verifying both integrity and authenticity, which will not protect against a Watering Hole attack, where the vendor's website has been compromised and both the software and the integrity check are likely to be compromised. However, we note that the majority of vendors use their websites for software downloads and include the hashes for integrity checks on those websites. Members have had difficulty in getting vendors to change their practices, which makes this requirement difficult if not impossible for Responsible Entities to comply with…Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third part, a vendor."

Likes 0	
Dislikes 0	

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

NRG recommends that the R3 and R4 technical/operation control requirements should be located in the associated standard to avoid misalignments or jeopardizing timeframes outline in the other standards such as patch management. For Example: R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4.

NRG requests clarification from SDT regarding what could/should an entity do if there is no process to verify the authenticity of software? In those cases, can an entity document their defense in depth strategies as a compensating measure? NRG recommends that SDT communicate in Measures that verification of authenticity could include a way to present in our processes other methods that may not actually be verification.

NRG recommends that SDT list ways that a Registered Entity can authenticate a source in the Measures section. NRG also recommends that SDT list that a Registered Entity should have a means to use putty, Debian, or things that don't have as tight of controls, (i.e. provide a checksum, and/or set a policy that they don't use open source code and requests clarification of how a Registered Entity would demonstrate that they had verified an authoritative source (i.e. open source) to the extent of what their capability would allow). For example, NRG recommends that SDT list examples in Measures section to include use of a layered approach of security and functional testing: For example start with a notification process, authenticity check of source, and use hash / checksum, then perform testing (but how does testing demonstrate authenticity? Answer – virus scan, etc (functional vs. security testing: A/V scan, logging, access, control). Lastly perform a scan from a vulnerability assessment tool. How does this prove integrity and authenticity of the software? NRG requests clarification in the standard requirement of when this requirement would become effective. NRG recommends that the SDT allow the Registered Entities additional time for vendor re-negotiations relating to supply chain for the purposes of enabling validation of integrity and authenticity of software and firmware.

NRG suggests that the R3 language should move to CIP-010. NRG requests clarification of whether testing is a valid form of verification. Additionally, we suggest the Requirement language to read as follows "Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being installed in operation on high and medium impact BES Cyber Systems". Each requirement should have a provision that allows an entity to accept the risk of selection a vendor that will not or cannot supply a control.

Likes 0	
Dislikes 0	

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

1. R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2. How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3. Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Does R3 allow the Entity to "accept the risk?"

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request "per system capability" wording for R3. Not all vendors provide a "golden hash" or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language "subject to procurement contract." There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

4. Additionally, R3 may hinder an entity's ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

5. Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where "obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan"

6. We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?	
Likes 0	
Dislikes 0	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	
Same as RoLynda Shumpert's comments from SCE&G: *SCE&G agrees with the concerns and questions raised by the Edison Electric Institute (EEI), including the following:* *"Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls. For example, the language could allow a Responsible Entity to use a vendor's website for verifying both integrity and authenticity, which will not protect against a Watering Hole attack, where the vendor's website has been compromised and both the software and the integrity check are likely to be compromised. However, we note that the majority of vendors use their websites for software downloads and include the hashes for integrity checks on those websites. Members have had difficulty in getting vendors to change their practices, which makes this requirement difficult if not impossible for Responsible Entities to comply with…Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third part, a vendor."*	
Likes 0	
Dislikes 0	

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	

We propose the SDT modify standard language based on Vectren's proposed language below:

R3:

Each Responsible Entity shall implement one or more documented process(es) for reviewing the vendor process for integrity and verifying authenticity of the following software and firmware, where a verification method is available from the vendor, before being placed in operation on high and medium impact BES Cyber Systems:

3.1 Operating System(s);

3.2 Firmware;

3.3 Commercially available or open-source application software; and

3.4 Patches, updates, and upgrades to 3.1 through 3.3.

Additionally, Vectren understands that due to the deadline for this standard there is not time for this now, but suggest that future revisions to the Supply Chain Risk Management standard, consider moving R3 to CIP-007 patching or possibly to CIP-010 change control to avoid "spaghetti" requirement as had existed prior to CIP V5.

Consider that future revisions format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered: **R3** - Concerns that not all vendor products will provide a method to check authenticity. Concerning patching, Vectren questions the ability of the utility industry to influence the vendor's contracting language. Please consider If EACMS and PACS are truly the intent of this standard. What steps will need to be taken to verify vendor is ensuring integrity of their business partners? Consider formatting CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples. Integrity is process internal to the vendor. Cannot verify integrity for each individual patch. What does the SDT consider a "secure central software repository"?	
Likes 0	
Dislikes 0	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Quintin Lee - Eversource Energy - 1	
Answer	No

Document Name	
Comment	
1) R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829. 2) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations 3) Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3	
Likes 0	
Dislikes 0	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
R3 applies whether revised contract terms and conditions exist or not, with no exception for vendor capability issues, technical feasibility, or situations where there is no vendor. It is also not clear whether changes that are not firmware or software versions or patches fall under the requirement. CenterPoint Energy requests that the phrase “where technically feasible” be added to Requirement 3. Furthermore, the Company believes verifying software integrity and authenticity as described in CIP-013 R3 belong in CIP-010 and recommends aligning the R3 sub-requirements to match the items in CIP-010 R1.	

It is not clear what an entity must do if the vendor will not or cannot assist by providing an authentication method. Having a verification requirement for R3.4, where not automatically supported by vendors, slows down the existing patch management process. This increases security risks by leaving systems unpatched against known vulnerabilities for longer periods and increases compliance risks for entities where dated mitigation plans must be used to document delays. Additionally, it is not clear whether secure boot capability, default on many Cyber Asset operating systems, is adequate (or even required) to demonstrate compliance with software verification requirement. CenterPoint Energy recommends that R3 be revised for flexibility and feasibility. It should also be moved to CIP-010 as these requirements would seem to fit as a part of existing configuration change management processes.	
Likes 0	
Dislikes 0	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Ballard Mutters - Orlando Utilities Commission - 3	

Answer	No
Document Name	
Comment	
OUC requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
CIP-013-1 Requirement R3 is written with an assumption that the supplier provides a mechanism in which verification of integrity and authenticity can be performed on software and firmware. These tools/mechanism may not always be available to the Registered Entity, and the Registered Entity may not have the power in which to force the supplier to provide a verification method. Consistent with currently approved and enforceable CIP Cyber Security Reliability Standards, ATC recommends the SDT consider adding language to provision for conditions where it is not technically possible to perform a verification in order to provide the flexibility needed to preclude an impossibility of achieving compliance. Additionally, the inclusion of "firmware" within the proposed language in CIP-013-1 R3 is an expansion in scope from the **first directive** in FERC Order No. 829 (P.2), which directed NERC to draft a new or modified Reliability Standard that "…should address the following security objectives, discussed in detail below: **(1) software integrity and authenticity;** (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."	

Additionally, CIP-013-1 Requirement R3 is simultaneously duplicative and additive with currently approved and enforceable CIP-010-2 Requirement R1 and the Applicable Systems within CIP-010-2 Requirement R1 Parts 1.1 – 1.5 as consequence of the broad reference to "high and medium impact BES Cyber Systems" without consideration of the construct of the CIP-010-2 Standard.

1. CIP-013-1 Requirement R3 Sub Requirements R3.1 – R3.4 are duplicative of CIP-010-2 Requirement R1 Parts 1.1 – 1.2, which obligates Registered Entities to develop and maintain a baseline of 'software' information for both high and medium impact BES Cyber Systems, where the types of software are effectively the same as what is being proposed.

o CIP-010-2 Requirement R1 Part 1.5 addresses the testing of changes to this 'software' and 'firmware' for high impact BES Cyber Systems, rendering Sub Requirement R3.1 – R3.4 superfluous and unnecessary. Consequently, Requirement R3.1 – R3.4 also creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-010-2 Requirement R1 Part 1.5. In its redundancy, it is at odds with the former efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

o CIP-010-2 Requirement R1 Part 1.5 has a provision to allow for the testing of this software and firmware in production where it is not technically feasible to perform testing in a test environment. CIP-013-1 R3 is effectively an expansion in scope to CIP-010-2 Requirement R1 Part 1.5 in its obligation to perform testing "…**before being placed in operation on a high** … …**impact BES Cyber System**". Any expansion in scope to access requirements or controls for high impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-010-2 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

o CIP-010-2 Requirement R1 Part 1.5 is not applicable to medium impact BES Cyber Systems. CIP-013-1 R3 is effectively an expansion in scope to CIP-010-2 Requirement R1 Part 1.5 in its obligation to perform testing "…**before being placed in operation on a… …medium impact BES Cyber System**". Any expansion in scope to access requirements or controls for medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-010-2 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

Likes 0	

Dislikes 0	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

Reclamation recommends Requirement R3 should instead require entities to review and update as necessary their supply chain risk management plan(s) developed in Requirement R1 at least once every 15 months.

Within each Requirement, the sub-requirements should distinguish between high, medium, and low impact BES Cyber Systems and other supporting systems. Reclamation recommends the implementation plan enforcement dates be staggered based on high, medium, and low impact for auditing purposes and to allow the associated risks and severity levels to be spelled out more clearly.

Likes 0	
Dislikes 0	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Rationale for Requirement R3:

The rationale language for R3 states, “The 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.” R1, R2, and the

Rationale for Requirement R3 do not specify the impact classification (High, Medium and Low) when referencing the BES Cyber System. R3 specifically states the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems.” IPC would like know if the inconsistent impact classification references were intended or were an oversight by the SDT.

R3

The requirement language for R3 states, “before being placed in operation on high and medium impact BES Cyber Systems.” R1, R2, and the Rationale for Requirement R3 do not specify the impact classification (High, Medium and Low) when referencing the BES Cyber System. R3 specifically states the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems.” IPC would like know if the inconsistent impact classification references were intended or were an oversight by the SDT.

The requirement language for R3 states, “Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware." IPC is concerned that the SDT developed a standard that requires Responsible Entities to “verify the integrity and authenticity” of software and firmware of which Responsible Entities have no oversight or control over what each vendor provides.

IPC does not feel CIP-013-1 is an appropriate standard to address R3. IPC believes this requirement belongs in CIP-007-6 or CIP-010-2 as R3 is related to patching or configuration change management. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-007-6 and CIP-010-2 address testing and verification of changes controls, which are typically performed by technical staff as they test, implement, and update systems.

Likes 0	
Dislikes 0	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA supports ERCOT's comments. CIP-013 R3 directly impacts baseline data and as such should be located within CIP-010.	
Likes 0	
Dislikes 0	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business or will not cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date.

2) The applicability of this requirement should be limited to high and medium impact BES Cyber Systems with external routable connectivity. This would align the standard with the applicability and risk-based approach of CIP-007 and CIP-010.

3) Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

4) Provide clarity for when a system is pre-loaded by a vendor and delivered to an entity. Is the entity required to verify software authenticity? If a computer is purchased from Dell, can Dell provide authenticity for all of the firm ware that is part of the system but not directly manufactured by Dell; i.e. system bios, sound system, network adapter, video controller.

Likes 0	
Dislikes 0	

Glenn Pressler - CPS Energy - 1

Answer	No
Document Name	

Comment

CPS Energy supports the comments provided by ERCOT and APPA

Likes 0	
Dislikes 0	

Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	
See EEI comments	
Likes 0	
Dislikes 0	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Colorado Springs Utilities (CSU) requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Leonard Kula - Independent Electricity System Operator - 2	

Answer	No
Document Name	
Comment	

Within the Rationale, the word “ensure” is inappropriate. Even good controls do not “ensure” a desired outcome. It should also state that “software being installed in the BES Cyber System was not modified or altered without the knowledge of the supplier AND the recipient or licensee. Consider replacement of “ensure” with “confirm”.

R1. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. To address these concern, The IESO request that the SDT consider the use of provisional language to protect Responsible Entities such as use of a TFE.

R1. The SDT should consider the use of “validate” instead of “verify” in this requirement.

R1. The SDT should address situations that are outside the usual upgrade and patch processes. This includes the obligations for signature updates, and where a vendor brings code onsite (binary or source code) that the entity is not allowed to review.

Likes 0	
Dislikes 0	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	

Seattle City Light requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the risk-based approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	

Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	
The NYPA Comments	
Likes 0	
Dislikes 0	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	

SMUD requests that the scope of R3 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity in alignment with the approach in existing CIP-007 and CIP-010.	
Likes 0	
Dislikes 0	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

Security Objective

Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language. Furthermore, operational checks to verify security controls are not adversely affected are covered in other CIP standards.	
Likes 0	
Dislikes 0	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA supports ERCOT's comments. CIP-013 R3 directly impacts baseline data and as such should be located within CIP-010.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	

Answer	No
Document Name	
Comment	

Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 0	

Dislikes 0	

Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	

Within the Rationale, the word “ensure” is inappropriate. Even good controls do not “ensure” a desired outcome. It should also state that “software being installed in the BES Cyber System was not modified or altered without the knowledge of the supplier AND the recipient or licensee. Consider replacement of “ensure” with “confirm”.

R1. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. To address these concern, The IRC and SWG request that the SDT consider the use of provisional language to protect Responsible Entities such as use of a TFE.

R1. The SDT should consider the use of “validate” instead of “verify” in this requirement.

R1. The SDT should address situations that are outside the usual upgrade and patch processes. This includes the obligations for signature updates, and where a vendor brings code onsite (binary or source code) that the entity is not allowed to review.

Likes 0	
Dislikes 0	

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No

Document Name	
Comment	

Requirement R3 and the associated guidance is not sufficient to explain the security objective this requirement is trying to address and the difference between integrity and authenticity controls.

The authenticity verification is already addressed in the procurement and vendor risk assessment process. Based on the vendor provided information in 1.1.5, 1.2 should identify the method or source to obtain the software that provides reasonable assurance of the authenticity of the vendor provided software.

Methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in test environment prior to installation on applicable assets, etc.

We recommend the following language for consideration by the SDT:

R3. Prior to installing new (1) operating systems(s); (2) firmware; (3) commercially available or open-source application software; and (4) patches, updates and upgrades to these, use one or more documented method(s) to minimize the risk of adversely or unintentionally modified software.

Requirement Placement (CIP-010)

Requirement R3 may also fit better within CIP-010 (e.g., after R3, Part 3.3) since it is more of an operational security control. However, the security objective for this requirement is focused on risk the vendor may introduce by delivering software that has been altered before or during transit to the Responsible Entity so keeping it in a separate, supply chain standard may also make sense. Also, to implement R3, Responsible Entities will likely need to work with the vendor during procurement (R1 and R2) to ensure that they can meet R3.

Verifying integrity and authenticity may also not be possible. This requirement should be about minimizing risk and recognize that the Responsible Entity may not be able to be verify that all risk has been eliminated, especially since the risk is from a third party, a vendor.

Likes 0	
Dislikes 0	

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

GTC disagrees with the proposed requirement. CIP-013-1 R3 requires actions to be taken by the Responsible Entity that are outside of the supply chain context. Paragraph 45 of Order No. 829, specifies this objective of software integrity and authenticity should be applied to "The Plan" identified in the core directive in the context of addressing supply chain management risks. The SDT has chosen to identify controls in R3 that are executed only as part of the day-to-day management of BES Cyber Systems. These controls fail to effectively address the security objective of addressing software integrity and authenticity, will have minimal security value, are administratively burdensome on industry, and are inconsistent with the supply chain context. SAFECode's (http://www.safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf) Software Integrity Control's whitepaper outlines controls that effectively address software integrity and authenticity. Nearly all of these controls must be implemented by the vendor. As such, Responsible Entity's should have the flexibility to require the vendor to provide software assurance through contractual means. Such as "supplier provides customer ways to differentiate genuine from counterfeit software"

Unfortunately, the SDT has not provided controls that effectively address software integrity and authenticity and has instead focused its control as demonstrated by the language in the measure on ensuring the "entity performed the actions." In order to provide entities the flexibility to effectively address the security risks associated with the supply chain, we respectfully request that the SDT revise its draft standard to be more in line with the framework identified in FERC Order 829. Our recommendation, consistent with our response to question 1, is as follows

GTC recommends the SDT reconsider relocating the attributes of R3 in a manner that addresses the security objective to "The Plan" specified in R1 to align with the FERC Order. This would allow the Responsible Entity to handle contractually with the vendor i.e. "supplier provides customer ways to differentiate genuine from counterfeit software (such as digital signatures)". Our recommendation is consistent with our response to question 1, which is summarized as follows:

See GTC's comment for Question #1.

Upon close review of FERC's directives summarized beginning on paragraph 43 through paragraph 62, the Order essentially directs this new Standard as outlined:

Paragraphs 43 – 45:

R1: Develop a plan to include security controls for supply chain management that address controls for mitigating Supply Chain risks to hardware, software, and computing and networking services which are intended to support Bulk Electric System operations; that include the following four specific security objectives in the context of addressing supply chain management risks:

R1.1 Security objective 3 (*information system planning*)

R1.2 Security objective 4 (*vendor risk management and procurement controls*)

R1.3 Security objective 1 (*software integrity and authenticity*)

R1.4 Security objective 2 (*vendor remote access*)

Paragraph 43:

R2: Implement the plan specified in R1 in a forward looking manner.

Paragraphs 46 - 47:

R3: Review and update, as necessary its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months

R3.1 Evaluation of revisions…

R3.2 Obtaining CIP Senior Manager or delegate approval.

Paragraphs 48 – 50:

FERC prescribes the various ways to address the first objective to the plan. Paragraphs 51 – 55: FERC prescribes the various ways to address the second objective to the plan. Paragraphs 56 – 58: FERC prescribes the various ways to address the third objective to the plan. Paragraphs 59 – 62: FERC prescribes the various ways to address the fourth objective to the plan. FERC goes on to respond to comments on Existing CIP Reliability Standards, beginning with paragraph 71, "while we recognize that existing CIP Reliability Standards include requirements that address aspects of supply chain management, we determine that existing Reliability Standards do not adequately protect against supply chain risks that are within a responsible entity's control. Specifically, we find that existing CIP Reliability Standards do not provide adequate protection for the four aspects of supply chain risk management that underlie the four objectives for a new or modified Reliability Standard discussed above." FERC summary continues to focus on CIP-013-1 being limited to aspects of supply chain risk management.	
Likes 0	
Dislikes 0	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

The NERC Entity is the customer of the hardware supplier and software supplier, not the designer, manufacturer and developer of what is being procured. As such, the Entity can only clearly state what they want the hardware and software to do – at a high level, likely derived from what the vendor said there product could do, along with the expectation that the product will be "bug free". But the Entity should not be expected to have the expertise and tools to "verify the integrity and authenticity of software and firmware". Integrity and authenticity can only be assured by each link backwards in the Supply Chain, and collectively that will only happen if each link of the Supply Chain agrees to control their link. CIP-013 is not in a position to impose those controls on the entire Supply Chain, but only on the end customer - NERC Registered Entity. That said, software and firmware should be expected to be checked for proper "functionality" by the Registered Entity, per past CIP practice.	
Likes 0	
Dislikes 0	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No

Document Name	
Comment	
This Standard, and therefore this Requirement needs to be squarely focused on the vendor product or service being procured and not on the categorization of a BES Cyber System. Requirement R3 should not be limited to High and Medium Impact BES Cyber Systems. A SEL-421 is a SEL-421 and the same risks of procurement, including firmware updates, apply to all SEL-421s impacted regardless of where they are deployed. Software/firmware updates are often acquired once and widely deployed. This is especially true in the substation environment where the exact same firmware release will be used to update Medium and Low Impact relays.	
Likes 0	
Dislikes 0	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No

Document Name	
Comment	

1) R3 creates confusion and possible double jeopardy with CIP-007 R2 and CIP-010 R4 part 1.4.4. Recommend moving R3 into these Standards/Requirements. This modification to CIP-007 and CIP-010 addresses FERC order No. 829.

2) How does the SDT propose that the responsible entity handle R3 for existing equipment when the vendor is out-of-business, is unable to cooperate, or is unwilling to cooperate? This equipment may have been purchased prior to the implementation of CIP-013 but not put in services until after the effective date. Recommend rewording this Requirement to allow exceptions for these situations

3) Request clarification (in the Standard) on how the SDT expects current and past contract negotiations to impact R3

Does R3 allow the Entity to "accept the risk?"

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

· Request "per system capability" wording for R3. Not all vendors provide a "golden hash" or other mechanism to validate.

· To be consistent with not requiring R1.2.5 we suggest adding the language "subject to procurement contract."

To be consistent with not requiring R1.2.5, we suggest adding the language "subject to procurement contract." There should be provisions to allow an entity to accept the risk of selecting a vendor that will not or cannot supply authentication.

Additionally, R3 may hinder an entity's ability to meet the 35-day patch window in CIP-007-6 R2.2 and R2.3. In the case of a non-cooperative vendor, entities will be left in a position of choosing to violate CIP-013, R3 or CIP-007, R2.

Is R3 the implementation of R.1.2.5? Should there be more explicit tie-ins? Seems to be in conflict with provision in R1 where "obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan"

We request clarification on relationships with resellers. Is verification of integrity and authenticity adequate from the reseller? Or does validation have to reach back to the original manufacturer?

Likes 0	
Dislikes 0	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
For a smaller CIP applicable medium impact BES Cyber System, we apply between 5,000 and 7,000 patches a year. The only feasible means for us to apply any meaningful integrity check is through automated, cryptographic mechanisms. This is a good practice, which should be followed, but we haven't found a good adoption rate by the Vendors developing the software. Even still, authenticity controls do very little without better software development lifecycle controls in place by the vendor. Additionally, the poor record of Certificate Authorities to control certificate validation should be raised. The cost of putting a process like this in place involves a heavily centralized procurement team and the time to research a large number of vendor practices pertaining to verification. We do not believe the risk reduction justifies this very costly requirement. We propose meeting the FERC directive through R1 and dropping this Requirement altogether.	
Likes 0	
Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	

Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
The NERC Entity is the customer of the hardware supplier and software supplier, not the designer, manufacturer and developer. As such the Entity can only clearly state what they want the hardware and software to do – at a high level, likely derived from what the vendor said it could do, plus expecting that it will be "bug free". But the Entity should not be expected to have the expertise and tools to "verify the integrity and authenticity of software and firmware" – that is required to be ensured by each step back in the Supply Chain, and that will only happen if each link of the Supply Chain agrees to control their link. CIP-013 is not in a position to impose those controls on the Supply Chain, but only on the end customer. Software and firmware should be expected to be checked for functionality by the Entity.	
Likes 0	
Dislikes 0	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No

Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes this Requirement is already covered in CIP-007. Having a CIP-013 requirement, that if violated, opens the door to double jeopardy (a finding in CIP-013 would also lead to a finding in CIP-007). There is no need for this Requirement. If there are additional requirements that must be identified, then CIP-013 is not the place for it, CIP-007 is a more appropriate place.	
Likes 0	
Dislikes 0	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No

Document Name	
Comment	

Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 3. In addition, we offer the following comments:

Ambiguous Language – "integrity" and "authenticity"

The crux of the Requirement is to develop and implement plan(s) that address verification of the "integrity" and "authenticity" of operating systems, firmware, open-source software, and certain patches and upgrades prior to use. Without defining or providing a framework as to what "integrity" and "authenticity" mean, the terms are not measurable for CMEP purposes.

We suggest the Requirement include language that points to established and accepted security frameworks and standards. We offer the following alternative language:

R3. Each Responsible Entity shall manage its Cyber Asset Systems supply chain informed by well-established and accepted cyber security frameworks and standards for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems:

Likes 0	
Dislikes 0	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	

Concur with EEI's Position	
Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
see APPA's comments, with which SVP agrees.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
R3 – line 2 – for clarity purposes NRECA recommends removing "software and firmware."	

Additionally, to the extent possible, NRECA recommends that this requirement should be incorporated into CIP-007 R2 or CIP-010 R1. This is a System Security Management requirement and belongs in the appropriate location. CIP-013-1 and R3.1-R3.4 are all components of the CIP-010 baseline. Placing this topic in a separate standard and requirement creates compliance confusion.	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE's testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets,

etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.	
Likes 0	
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE's testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets,

etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.	
Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	
We don't believe it is reasonable to expect entities to be able to "verify" the integrity and authenticity of software and firmware in all cases. We can attempt to minimize the risk and/or provide reasonable assurance that we have received what was intended. There also needs to be a recognition of the many varied ways that updates and installations of software and firmware might be done most effectively, including the use of automated solutions.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.

In addition, the concerns expressed by EPE in response to Requirement 1 with respect to the proposed verification requirements also applies with respect to Requirement 3. Requiring a Responsible Entity to have a process to address verification is different from making a Responsible Entity responsible for software and firmware verification. EPE has had experiences in the past where the developers/vendors of software products provided to EPE products that they considered authentic and to have integrity. EPE's testing in a strong test environment (before the products were placed in service) did not reveal any errors, yet, as the products were placed in service, errors were revealed that could not be explained *by the software developers themselves*. Under the new standard, as worded currently, would this experience create an instance of noncompliance? If so, how would a Responsible Entity avoid being noncompliant in a situation in which the product vendor created the product and still could not predict or explain the error?

As EEI explains in its comments, methods to minimize the integrity risk is determined based on the vendor and Responsible Entity's capability, and could include hash verification, vendor program review with acceptable assurance of good SDLC process and defined distribution source, through operational and security testing of software in a test environment prior to installation on applicable assets, etc. If a Responsible Entity may satisfy its compliance responsibilities for integrity verification through such methods, the requirement should be recrafted with language that makes this clear to the Responsible Entity.

Likes 0	
Dislikes 0	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT supports the IRC comments on this question and offers the following supplemental comments.

ERCOT recognizes the need for the concepts contained in Requirement R3. However, ERCOT disagrees with the placement of the requirement in a new standard. Since this requirement is applicable to only high and medium impact BES Cyber Systems, it should be placed within CIP-010. The requirement directly impacts the baselines that have been established within CIP-010 R1. The SDT could insert a new part between existing Parts 1.1 and 1.2 in that standard. The new part could use the following language: "For any updates or patches that that deviate from the existing baseline configuration, verify the authenticity and integrity of the update or patch." As mentioned previously, in developing the CIP Version 5 standards, the SDT performed extensive work to ensure that all requirements related to a particular subject were included in one standard instead of being spread across multiple standards. The proposed language will disrupt that framework. Including the requirement in CIP-010 will ensure that a single standard captures all parts of the change process, including inventory (Part 1.1), validation of the code (NEW), authorization of implementation (Part 1.2), update of the inventory (Part 1.3), and testing of the change (Parts 1.4 and 1.5). This approach would give Responsible Entities a complete view of what is required from the start to the end of a change. It also prevents entities from keeping separate inventories to meet the CIP-010 requirement and the CIP-013 requirement.

Additionally, ERCOT requests guidance on how to demonstrate compliance when using automated solutions to obtain the most current patches applicable to their systems. In large environments, these automated solutions are critical to meeting the timing obligations of CIP-007 R2. Inserting the manual step of verifying integrity and authenticity of updates and patches can prevent the use of these solutions that entities have invested in and rely upon for addressing security risks and regulatory obligations. If it is intended that the entity may simply document the source used by these solutions, it would be helpful to put such clarifying language in the requirement.

Additional use cases for the SDT to consider in developing guidance include: (1) how signature and pattern updates are contemplated within the requirement since these are not updates to the operating system, software, or firmware noted, (2) instances when code is packaged and mailed to an entity, (3) software and firmware that are part of a vendor black-box type of appliance solution where the entity has no visibility to the code on the device, and (4) vendors bringing code onsite that the entity is not allowed to review. Any of these cases could present an obstacle to strict compliance with the draft standard language.

As with Requirement R1, this requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. The drafting team should address situations in which vendors will not or cannot provided the levels of service mandated by this requirement. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms

otherwise required by R3. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)	
Likes 0	
Dislikes 0	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company disagrees with the direction the proposed R3 requirement is taking. Given our previous comments under R1 regarding the proper scoping of this new Standard to the "Supply Chain" time horizon, actions proposed to be required under R3 fall outside of that time horizon where the controls are applicable to BES Cyber Systems, which are not yet designated or commissioned as such. Additionally, R3 requires the development of "one or more documented processes" that are in addition to "the plan(s)" required in R1; Southern recommends maintaining the proper scoping of this Standard by moving the components of R3 under R1 to be addressed by the Responsible Entity in "the plan(s)."

If R3 is not consolidated under the R1 requirements for "the plan(s)" to be applicable within the Supply Chain time horizon, then Southern provides the following recommended edits to maintain vital consistency with existing requirements under CIP-010 R1.1. There is firmware in every video card, mouse, hard drive, etc. that is NOT the objective of the requirements in this Standard, but could, without the qualification provided below, be included. The addition under R3.2 also provides vital consistency with CIP-010 R1.1 so we aren't maintaining different baseline configurations on all of our systems because of slightly different wording in the two Standards.

In this situation where very similar requirements in two different standards create additional administrative burden on entities, the SDT needs to recognize and address the delays that the proposed R3 requirements will have on the existing requirements under CIP-007-6 R2 (Patch Management). The burden of verification of integrity and authenticity of software and firmware in front of applicable requirements

for determining availability, applicability, and conducting deployment of security patches within 35 day cycles will make those existing requirements under CIP-007-6 R2 unmanageable and will increase the administrative burden of creating patch mitigation plans as a result of competing Standards.

Modify R3 language as follows:

R3. Each Responsible Entity shall implement one or more documented process(es) that addresses the verification of the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

3.1 Operating System(s) or firmware where no independent operating system exists;

3.2 Commercially available or open-source application software intentionally installed; and

3.3 Patches, updates, and upgrades to 3.1 and 3.2.

Likes 0	
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Eric Ruskamp - Lincoln Electric System - 6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
We agree with this in principal, but this requirement will be extremely difficult to implement and ensure compliance. Currently, numerous vendors do not provide digitally signed patches (Microsoft is notorious for this) or other hashes to verify that a file was not modified. The ability to verify 100% of all software and files will be impossible until vendors are required to implement digital signatures. This can be done via contracts, but it will take time. We highly recommend that the requirement be changed to allow for the fact that software may not be able to be verified and that as long as an entities process checks for this that it is still valid to install with risks.	
Likes 0	
Dislikes 0	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

This appears to be a reasonable approach to meeting the FERC directive.	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
What other measures or documented evidence should be expected by the Regional Entities when evaluating R3 at audit? An entity could leverage existing CIP-010-2 R1 (3.1-3.3) baseline controls and CIP-007-6 R2 patch management (3.4) controls to support the integrity and authenticity of software and firmware as specified in the CIP-013-1 R3 requirement. However, since the baseline configurations are	

developed and managed at the BCS level, it is possible that a change to the baseline configuration(s) of a vendor supplied system may not trigger a change to the corresponding baseline configuration for the BCS to which the system(s) is assigned. Therefore, relying on changes to the baseline configuration(s) may not (by itself) be a reliable control to determine if changes were made to a new vendor-supplied system. In such cases, the addition of a simple control (an extra check for new vendor-supplied systems) integrated into an entity's existing CIP-010-2 program would suffice to address the issue.	
Likes 0	
Dislikes 0	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
1. We favor industry accepted methods to address software authenticity such as digital signatures that are consistent with other critical sectors.	
Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

BPA proposes that to truly isolate the production systems from compromised software or firmware more prescriptive language than 'before being placed in operation' is required. BPA recommends the SDT develop language to address a supplier that is unwilling or able to support the requirement.	
Likes 0	
Dislikes 0	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS notes that Requirement R3 requires documented processes for verifying the "integrity and authenticity" of software and firmware before being place into operation and that such language may result in redundant verifications and processes. In particular, software, firmware, etc. are often verified when they are received from the vendor and "incubated" on low risk systems before being pushed to BES Cyber Systems. To avoid the need to "re-verify" these updates after incubation, but prior to placement in production on BES Cyber Systems, AZPS requests the following change to Requirement R3, '…verifying the integrity and authenticity of the following software and firmware ***being placed in operation on high and medium impact BES Cyber Systems***, **when received**'. Additionally, Requirement R3 addresses the verification of integrity and authenticity of software and firmware; however, it does not address the likelihood of a vendor's inability or unwillingness to comply. AZPS requests clarification of whether an inability to verify would be considered a failure to implement the process if verification is not possible due to vendor inability or unwillingness.	
Likes 0	
Dislikes 0	

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • The way this requirement is written, it may not be possible to perform a technical verification of software integrity and authenticity. How does the standard drafting team expect registered entities to address this if it cannot be done in a technical manner? • Requirements R1 and R2 do not require the registered entity to go back and revise previous contracts. In order to comply with this requirement, R3, changes to past contracts / vendor service agreements may be required. Alignment is needed between R1, R2, and R3.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	

We recommend the SDT address virtualization and CIP Exceptional Circumstance with respect to this requirement aligned with project 2016-02. Also please see our earlier comments with regards to redundancy between R3 and R1.2.5.	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	
Document Name	
Comment	
Suggest striking the word “associated” from the phrase “software, firmware, and associated patches”.	

Basin Electric recommends adding language to address potential Technical Feasibility Exception (TFE) such as: R3. Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware**, where technically feasible,** before being placed in operation on high and medium impact BES Cyber Systems: In R3.2, "Firmware" is already included in R3 which is redundant in R3.2. Basin Electric recommends R3 be written as a general Requirement with specifics in the sub Requirements. There are a lot of parallels between these requirements and the requirements already required in CIP-007 R2 patch management controls. Basin Electric would rather see these obligations integrated into CIP-007. The rationale explains the obligation for this requirement starts in the operate/maintain phase of the life cycle, but the timing/life cycle language is not included in requirement. Basin Electric suggests modifying the requirement to include clarification of when the obligation starts. Perhaps add language to the front of R3 such as: "For Cyber Assets in production…"	
Likes 0	
Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	

4. The SDT developed CIP-013-1 Requirement R4 to address the Order No. 829 directive for entities to address logging and controlling third-party (i.e., vendor) initiated remote access sessions including machine-to-machine vendor remote access to BES Cyber Systems (P 51) as it applies to high and medium impact BES Cyber Systems. Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Summary Consideration. The SDT thanks all commenters. The SDT removed this requirement from CIP-013-1 as recommended by commenters and is addressing the directive by modifying existing CIP standards. The SDT sought input from the Project 2016-02 CIP Revisions SDT and developed Proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the directive. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement as the objective of Part 2.4. The objective of Requirement R2 Part 2.5 is for entities to have the ability to rapidly disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

Specific comments and SDT responses are provided below:

Commenters stated that the directive should be addressed in other CIP standards. The SDT developed revisions in CIP-005-6 to address risks and reliability objectives from Order No. 829 dealing with vendor remote access. The SDT based revisions on input from the Project 2016-02 CIP Revisions SDT.

Commenters stated that Responsible Entities need flexibility to account for technical feasibility or vendor capability. The new requirements in CIP-005-6 require entities to have one or more methods for determining active vendor remote access sessions, and one or more methods for disabling active vendor remote access. The SDT believes Responsible Entities can meet these objectives and will not need exceptions based on vendor capability.

Commenters recommended clarifying or changing the assets in scope for the requirement; or using a table for clarity. The revised requirement in CIP-005-6 is clearly drafted using a table format. The SDT believes the scope of High and Medium BES Cyber Systems and associated PCAs is consistent with other remote access requirements, and that this will appropriately address the reliability objective for vendor remote access as specified in Order No. 829.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

As written, R4 is more appropriately addressed in other existing standards, CIP-004 for authorization, CIP-005 for remote access, CIP-007 for logging, and CIP-008 for response. Furthermore, it confuses the expectation of all these standards from an audit perspective by duplicating or undermining existing requirements. Authorization for interactive remote access is already covered in CIP-004 R4. Logging and monitoring of access to an Intermediate System or BES Cyber Asset is already covered in CIP-007 R4. If an entity requires separate evidence for those standards and CIP-013 R4, this could present a double jeopardy situation for compliance where an entity can be audited and penalized twice for similar requirements if a Regional Entity does not find their methods of compliance satisfactory.

Controlling remote access, including vendor remote access, is already addressed in CIP-005 R1 and R2 so CIP-013 R4 will overlap with those existing requirements. CenterPoint Energy recommends changing “system-to-system remote access with a vendor” to “vendor initiated system-to-system remote access” and modifying existing requirements if necessary, rather than including the requirements in CIP-013.

R4.3 is part of an entity's incident response plan, and should be in CIP-008. R4.2, R4.3 sub-requirements both need clauses for per Cyber Asset capability or technical feasibility exceptions.	
Likes 0	
Dislikes 0	
Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

2) Recommend that this Rationale needs to be updated from "machine-to-machine" to "system-to-system" for consistency

3) The first sentence of R2 is broader than the second sentence. The first sentence is "Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems." The second sentence is "The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):" Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

4) Request guidance. "Vendor-Initiated" could be considered a single word and not associated with the proposed definition of "vendor".

5) Recommend changing R4.3, from "Disabling or otherwise responding to unauthorized activity during remote access sessions" to "Disabling or otherwise responding to *detected* unauthorized activity."

6) The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.	
Likes 0	
Dislikes 0	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
We propose the SDT modify standard language based on Vectren's proposed language below:	

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we

must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.	
Likes 0	
Dislikes 0	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	
Same as RoLynda Shumpert's comments from SCE&G: *SCE&G agrees with EEI in its assessment regarding R4:* *"The use of "activity" in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as "escorted cyber access." In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions… We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3."*	
Likes 0	
Dislikes 0	
David Rivera - New York Power Authority - 3	

Answer	No
Document Name	
Comment	

1. R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

2. Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

3. The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

4. Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

5. Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6. The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

7. Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

8. R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

9. For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3. 10. This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs. 11. Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2. 12. SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says "during the remote access session," which may not reasonable amount of time since this is a real-time action.	
Likes 0	
Dislikes 0	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG suggests that R4, Section 4.1, Section 4.2, Section 4.3 language be moved to CIP-005. Since this is interactive remote session specific, NRG recommends moving all of these requirements into CIP-005 because of the implied real-time monitoring and logging requirements. Even though there are monitoring requirements in CIP-007, the monitoring requirements of CIP-007 are more forensic in nature. Various vendors and entities will likely want to implement individualized solutions to manage this requirement which will become administratively burdensome to the industry. These varied solutions can also present more ports being open (a reliability /security risk) to High and Medium	

BES Cyber Systems which could lessen reliability. NRG recommends that scope of this requirement should be for High and Medium with ERC BCS.

NRG requests that the SDT provide clarity that "system-to-system" is equivalent to "machine-machine" and what does it mean (i.e. application interface vs. laptop/server level). NRG recommends reference to the OSI layers. The R4 rationale appears to be inconsistent with the FERC directive regarding "machine to machine". NRG requests clarification of whether the rationale / intent of "system-to-system" is meaning that a direct machine to machine interface is needed or that it needs to go through an intermediate or third host (jump host). NRG requests that the term "vendor" be defined to clarify intent of meaning a company or an individual (in the context of interactive remote access).

In the implementation plan for this standard, NRG recommends a staggered implementation plan for R1, R2 & , R5 being 15 calendar months. However, NRG recommends a 24-month implementation plan for R3 & R4would be needed for Registered Entities to manage this process on all impacted systems due to the need to re-negotiate processes with vendors (individualized solutions).

Likes 0	
Dislikes 0	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

SCE&G agrees with EEI in its assessment regarding R4:

"The use of "activity" in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as "escorted cyber access." In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the

Responsible Entity would not be able to recognize inappropriate actions… We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3."	
Likes 0	
Dislikes 0	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Interactive Remote Access controls are defined in CIP-005 and in CIP-007. These requirements are duplicative and create the possibility of double-jeopardy for non-compliance. In addition, CIP-004-6 R4 Part 4.1.1 specifically addresses electronic access. Dominion is of the opinion that CIP-013-1 should concentrate on supply chain obligations for system-to-system communications which isn't addressed under the existing CIP standards. Operational requirements, such as the proposed R3, should be added to the appropriate CIP standard.
- Dominion recommends removal of Part 4.2. Complying with the logging requirement could degrade system performance to the point where the BES reliability would be negatively impacted. Additionally, the monitoring requirement further degrades the performance, and may not be technically feasible.
- If Part 4.2 is retained, the requirements should state the minimum criteria for logging and monitoring unauthorized access, as currently outlined in CIP-007-6 Part 4.1.
- The terms "access" and "activity" as used in the proposed CIP-013-1 need to be defined.
- Read only access should be excluded from the final requirement based on definition of Interactive Remote Access.

- Dominion recommends the removal of Part 4.3 Disabling or otherwise responding to unauthorized activity during remote access sessions seems to imply an on-going monitoring of active connections to a degree that's not technically feasible.
- If Part 4.3 is retained, we recommend that the minimum criteria for logging and monitoring be limited to disabling what has been detected. Dominion recommend the following language to achieve this goal:

4.3: Disabling or otherwise responding to detected, logged, and monitored unauthorized activity during remote access sessions.

- Dominion recommends creating a definition "system-to-system remote access" in the NERC glossary. Using a broad undefined term can lead to inconsistent results.

Likes 0	
Dislikes 0	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining "unauthorized activity" if that is not changed to "unauthorized access".

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	

Specific operational cyber security controls are best addressed as revisions to CIP-002 through -011.

Refer to EEI comments on R4 which point out overlaps to existing requirements in CIP-004, -005 and -008.

We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources.

We further point out the FERC Order 829 has directed revisions to remote access (for vendors) by Sept. 2017 which is before FERC's Order 822 P64 directive to NERC for a CIP version 5 remote access controls effectiveness study is even due. The remote access controls effectiveness study is not due till June 30, 2017.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we

must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.	
Likes 0	
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	

The proposed Requirement creates significant overlap with existing CIP Requirements. Requirement R4, as well as Requirements R3 and R5, should be modified so that CIP-013 only addresses those aspects of software integrity and authenticity (R3), remote access (R4), and authenticity and remote access for low impact BES Cyber Systems (R5) not covered by other Standards. Exelon understands that the timeframe dictated by FERC in Order No. 829 does not allow for revisions by this SDT to the relevant Standards that address these topics. However, overlap between the Standards should be avoided as much as possible to avoid double jeopardy concerns in the event of potential non-compliance with CIP-013 R3, R4, and R5.

For example, Exelon's review of the draft CIP-013-1 Standard indicates the following areas of overlap:

• CIP-013-1 R3.1 through R3.4 require authentication of operating systems, firmware, software, and patches. However, the configuration change management requirements under CIP-010-2 R1 already require that the configuration of operating systems, firmware, and software be carefully tracked such that counterfeit operating systems, firmware, software, and patches would be identified (e.g. a software difference would be identified as a change from the existing baseline configuration) and would be evaluated.

• CIP-013-1 R3.4 requires authentication of patches, updates, and upgrades, but CIP-007-6 R2.1 already imposes a patch management process for tracking, evaluating, and installing cyber security patches, including the identification of patching sources. Part of the

identification of patching sources under CIP-007-6 is the verification that those sources are authentic as CIP-013-1 R3.4 would appear to require.

• CIP-013-1 R4.1 requires authorization of remote access to certain BES Cyber Systems by the vendor. CIP-004-5 R4.1.1 already contains a process for authorizing electronic access to these assets by all personnel, including vendors.

• CIP-013-1 R4.2 requires logging and monitoring or remote access sessions. CIP-007-6 R4.1 already requires logging of all access and CIP-007-6 R4.2 requires alerting for any malicious code as well as any “security ecent that the Responsible Entity determines necessitates an alert.”

• CIP-013-1 R4.3 also requires responding to detected unauthorized activity, and because unauthorized activity on a BES Cyber System would constitute a “Cyber Security Incident,” CIP-008-5 already requires a response to such incidents.

• CIP-013-1 R5 requires a process for controlling vendor remote access to low impact BES Cyber Systems. This overlaps with CIP-003-6 Attachment 1 Section 3 which already requires electronic access controls for low impact BES Cyber Systems the limit access to necessary access.

The draft CIP-013-1 requirements should be modified so that overlaps are removed and that CIP-013-1 only addresses vendor issues not covered within existing Standards. To the extent the SDT believes there is no overlap between CIP-013 and the existing CIP Standards, the SDT should explain in each instance where the CIP-013 Requirement ends and the other CIP Requirement begins. In the absence of such guidance, a Compliance Monitoring and Enforcement Process could conclude that a particular instance of non-compliance with CIP-013 is also a simultaneous violation of another Reliability Standard, doubling the available penalty range. For example, draft CIP-013-1 R4 requires the Responsible Entity to authorize remote access by vendor personnel. The current CIP-004-6 R4.1.1 also requires authorization of vendor personnel to have electronic access. Therefore noncompliance with CIP-013-1 R4 would appear to, per se, constitute noncompliance with CIP-004-6 R4.1.1. Such double jeopardy serves no apparent reliability purpose. If the current CIP-013-1 R4 language is adopted as-is, the SDT should explain how its requirements differ from those under CIP-004-6 R4.1.1.

Finally, Exelon suggests that R4.3 may be difficult to accomplish in all cases and is overly prescriptive and thus should be removed from CIP-013. Order No. 829, P.52 references the Ukraine event and 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.” There are alternate methods to address this threat. First, two factor identification methods can be used to mitigate the risk of stolen credentials. Second, the use of WebEx or Skype sessions or active control of

vendor access (i.e. opening a port for access only when needed) can be used to address emergent issues and reduce the need for remote persistent sessions.	
Likes 0	
Dislikes 0	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	
Comment	

We propose the SDT modify standard language based on Vectren's proposed language below:

R4.

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) machine-to-machine remote access with a vendor(s):

4.1 Authorization of remote access by the Responsible Entity;

4.2 Log and review vendor remote access;

4.3 Disabling or otherwise responding to unauthorized access during remote access sessions.

Consider removing R4 and refer to CIP-005 R2 regarding Interactive Remote Access. If this is not an option, Vectren offers the following suggestions:

Consider defining system-to-system access (is this aka machine-to-machine)? See page 13 of Technical Guidance and Examples, paragraph #9.

Consider direct application access servers, such as those that deliver anti-virus signature updates, are not considered in scope.

Consider defining “unauthorized activity” if that is not changed to “unauthorized access”.

For future consideration, format CIP-013 into a table format similar to CIP-008 & CIP-009 for clarity. Expanded comments could then be moved to Technical Guidance and Examples.

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R4

This requirement is too broad to implement or audit and, therefore, outweighs the purpose of the regulatory efforts. Same question as in R1.2.6 concerning anti-virus signature updates. Unauthorized activity is not defined. This is open to interpretation such as to include a user opening files they should not be viewing, or looking at settings that are not related to the task at hand. This could also be interpreted that we must monitor every move, such as monitoring only through a WebEx while the vendor is accessing the system. Auditor could interpret this in many ways.

Likes 0	
Dislikes 0	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

We suggest that Requirement R4 Section 4.1 language be moved to the CIP-004 Standard. The group feels that CIP-004 Part 4.1 already handles access controls in that particular Cyber Standard. Additionally, we feel that a potential conflict may exist between CIP-013 Requirement R4 and CIP-004 Requirement R4 if this Requirement stays in its current position.

As for Section 4.2 language being moved to the CIP-007 Standard, our group feels that the CIP-007 Standard already addresses logging.

Finally, we suggest moving Section 4.3 Language to the CIP-005 Standard because, we feel that the CIP-005 Standard already addresses interactive access to BES Cyber Systems.

Likes 0	
Dislikes 0	

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Authorization of remote access to BES Cyber Systems (Part 4.1) is already addressed by CIP-004-6 R4 for user-initiated remote access and implicitly by CIP-005-5 R1 Part 1.3 (“Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”) for machine-to-machine access. It should be deleted.

Likes 0	
Dislikes 0	

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See Comments on Requirement R4 in attached file.	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	

Comment
R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829. The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard. R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written. After moving to CIP-005, R4.2 should be revised to say: “Capability to detect unauthorized activity; and” R4.3 should add the word “detected” before the term “unauthorized activity.” For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3. This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs. Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2. Suggest that this Rationale needs to be updated from “machine-to-machine” to “system-to-system.” SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.
Likes 0	

Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	
Comment	

R4 appears to be in parallel to requirements that already exist in CIP-004, CIP-005, CIP-007 and CIP-008. Basin Electric would prefer the requirements be integrated with the existing standards.

Basin Electric believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, Part 4.3 should be taken care of by complying with CIP-005-5 Part 1.3 which requires inbound and outbound access permissions which prevent unauthorized activity.

R4, Part 4.3 “otherwise responding” should be taken care of by complying with CIP-008-5 R2.

In the context of R1–R3, the term “vendor” appears to apply to a company as stated in the rationale section. In context of R4, the same term “vendor” now appears to mean individual personnel who represent a company. Clarity is needed on who this requirement actually applies to.

Likes 0	
Dislikes 0	

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Please refer to RSC- NPCC comments	
Likes 0	
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No

Document Name	
Comment	

- The scope of CIP-013-1 R4 appears to overlap with parts of CIP-005-5R1.3, R1.5, R2.1 - 2.3; and CIP-007 R4.1, R4.2, R5.7. (Both of the CIP-007 and CIP-005 requirements apply to High and Medium BCS and associated EACMS, PACs, and PCAs). However, the logging and monitoring requirements in CIP-007-6 R4.1, 4.2 specifically cite "per Cyber Asset capability" and "after-the-fact investigations."

o Additionally, the CIP-013 requirement indicates "Disabling or otherwise responding to unauthorized activity during remote access sessions." Not all technologies would have the capability of real-time cyber asset level user activity monitoring, needed to detect activity and disable sessions.

o CIP-013 R4 does not consider the variability of cyber asset capability. Not all technologies can support cyber asset level logging.

- A definition of "unauthorized activity" is needed. Note: existing processes in CIP-004 establish authorized activity for vendors, contractors, and employees, including: training, PRA, and access management. Security controls in CIP-005 and CIP-007 enforce the limits of those authorizations. Vendors who are granted specific access rights to remotely access systems are, by definition, authorized to perform certain functions. Jump-hosts, firewalls, user accounts, and application privileges already limit activity to permitted activity.

- "Machine-to-machine vendor remote access" should be defined, or the formal definition of "Interactive Remote Access" should be modified to include machine access.

- "Monitoring" should be defined. Suggested clarification is that monitoring includes information regarding the startup and termination of the connection, but does not include the capturing of user activity during the session.

Likes 0	
Dislikes 0	

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	
Comment	

SRP requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. SRP requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. SRP requests changing the language to "upon detected unauthorized activity".

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	
Comment	

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to "upon detected unauthorized activity".	
Likes 0	
Dislikes 0	
Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
CIP-013 R4.1 is duplicative of CIP-004 R4.3 as all persons already require authorization of electronic access to the systems in scope of this requirement. As entities will have to follow duplicate requirements in two different standards, CIP-004 and CIP-013, there is an increased likelihood of a violation. CIP-013 R4.2, Logging, monitoring, and alerting is already covered in CIP-007 R4.1 and R4.2. An additional requirement part in CIP-007 R4 would be the most effective place to meet this FERC expectation. As entities will have to follow duplicate requirements in two different standards, CIP-007 and CIP-013, there is an increased likelihood of a violation. CIP-013 R4.3 would be handled best as a component of CIP-007 R4 for detected inappropriate access. Alerting is already required by CIP-007 R4.2 and a simple additional step (requirement part) would require a response to the alert. The guidelines and technical basis should discuss use of intrusion prevention systems to meet this requirement without requiring significant additional compliance evidence.

Likes 0	
Dislikes 0	

W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	

Comment
I support the comments of Andrew Gallo at Austin Energy.

Likes 0	
Dislikes 0	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access. Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to "upon detected unauthorized activity".	
Likes 0	
Dislikes 0	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to "upon detected unauthorized activity".

Likes 0	
Dislikes 0	

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

R4 creates confusion and possible double jeopardy with other standards. Recommend modifying modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 address the FERC order No. 829.

Recommend that this Rationale needs to be updated from "machine-to-machine" to "system-to-system" for consistency

The first sentence of R2 is broader than the second sentence. The first sentence is "Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems." The second sentence is "The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a

vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to detected unauthorized activity.“

For R4.3, the “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Suggest changing to “detected unauthorized activity”.

Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

Likes 0	
Dislikes 0	

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. AE requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. AE requests changing the language to “upon detected unauthorized activity”.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	

PRPA requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. PRPA requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. PRPA requests changing the language to "upon detected unauthorized activity".

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

CHPD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. CHPD requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and

would be dependent on how the unauthorized activity was detected. CHPD requests changing the language to “upon detected unauthorized activity”.	
Likes 0	
Dislikes 0	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI supports the following comments from the MRO NSRF: “The NSRF believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4: R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1 R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1 R4, P4.3 should be taken care of by complying with CIP-005-5. Part 1.3 of CIP-005-5 requires inbound and outbound access permissions which prevent unauthorized activity.” Furthermore, AECI contends that the SDT should remove this requirement and address vendor remote access in the implementation of the supply chain risk management plan(s) as detailed in the requirement concepts proposed by AECI in Question 1. This concept will allow Responsible Entities to address the issue contractually with applicable vendors.	
Likes 0	
Dislikes 0	

Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	

Answer	No
Document Name	
Comment	
We request confirmation that vendor access does not include onsite staff augmentation contract resources. Clarification is also requested on whether "system to system" access applies to access that is "one-way" where the remote end conducts only monitoring activity and no control is possible. Can the procedure for access make distinctions for each method of monitoring each type of access, Interactive Remote, system to system with control and system to system for monitoring only? Finally, the term "unauthorized activity" is unclear. We recommend using the term "unauthorized access".	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Anthony Jablonski - ReliabilityFirst - 10

Answer	No
Document Name	
Comment	
The rationale section in Requirement R4 speaks to "machine-to-machine vendor remote access" while the actual requirement speaks to "system-to-system remote access with a vendor". ReliabilityFirst recommends the SDT use consistent language so that there is no confusion on terminology or definitions. Requirement R4 mentions high and medium BES Cyber Systems, but does not include their associated Electronic Access Control and Monitoring Systems (EACMs), Physical Access Controls(PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following modifications for consideration:	

Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems [and if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets]. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*	
Likes 0	
Dislikes 0	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends that the drafting team consider creating a definition for the terms “vendor” and “unauthorized activity”. Without clear expectations as to what is considered unauthorized activity, and further technical guidance on how to detect this type of activity, the Responsible Entity will not be able to determine what to look for to comply with R4.2, and will not know when to disable this activity to comply with R4.3. We request further clarification from the drafting team on what is meant by “*vendor-initiated Interactive Remote Access”.* Does this refer to access that originates from a non-Responsible Entity system? Also, does “*remote access*” apply in the instance where a non-Responsible Entity party accesses a BES Cyber System remotely to the ESP, but is originating on a network inside of the Responsible Entity’s infrastructure? Should the requirement language be revised to better categorize remote access as “external” remote access originating from a location that is not a Responsible Entity’s facility or location?	
Likes 0	
Dislikes 0	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Please consider consolidation of R4 requirements into CIP-005 instead of a separate requirement to assist REs who may utilized shared processes and systems for providing Interactive Remote Access, regardless of the origin of the remote access.	
Likes 0	
Dislikes 0	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
This risk should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-005 R2, CIP-004 R4, and CIP-007 R4. IID feels that there should be an exclusion comparable to a CIP Exceptional Circumstance (or Technical Feasibility Exception) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.	
Likes 0	

Dislikes 0	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

This seems not to be a supply-chain issue. It would seem that NERC's intent is to wrap-up order 829 into a single standard instead of modifying the existing standards (CIP-005 Requirement 2), where necessary, to address these weaknesses.

There should *most definitely* be a feasibility exception with respect to 4.2 and 4.3.

What does 'during remote access sessions' mean in 4.3? If the session is active, it would be prudent to expect immediate termination of the connection as the Guidance suggests – responding in a timely manner. Termination during a remote access session could imply a normal, or 'timed' termination of the connection, long after an intended response to unauthorized activity would ordinarily occur.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	

R4 is applicable to all BES Cyber Systems and, as applicable, EACMS PACS and PCA. The philosophy used by preceding CIP standard drafting teams has been to write any requirements for low impact BES Cyber Systems in Attachment 1 of CIP-003 R2. AEP believes this is a practice that results in a greater potential for compliance of all Responsible Entities. AEP recommends that the essence of R1 be rewritten to address the lower risk associated with low impact BES Cyber Systems and moved to CIP-003 R2 Attachment 1. In addition, CIP-013-1 R4 should be rewritten to be only applicable to high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	

R1.2.6 is duplicative of R4. These requirements should be made consistent, or one of them should be deleted. Much of R4 is already covered by CIP-005 (R1 and R2), CIP-007 (R4) and CIP-008. Requirements for a single topic should be consolidated within a single standard.	
Likes 0	
Dislikes 0	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The NSRF believes the following items will cause double jeopardy if there is a non-compliance action with the proposed R4:

R4, Part 4.1 is duplicative with CIP-004-6 R4, Part 4.1

R4, Part 4.2 is duplicative with CIP-007-6 R4, Part 4.1

R4, P4.3 should be taken care of by complying with CIP-005-5. Part 1.3 of CIP-005-5 requires inbound and outbound access permissions which prevent unauthorized activity.

Remove “disable or other responding” and replace with “ ”. Leave the options for response with the Register Entity.

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	

Comment

Southern Company strongly disagrees with the direction the proposed R4 requirement is taking, while recognizing the time constraints placed on the SDT to file a new or modified Standard addressing Supply Chain risks. As currently drafted, R4 carries significant overlap and repetition with existing CIP Standards, specifically with CIP-004-6 R4, CIP-005-5 R1, CIP-007-6 R4, and CIP-008-5 R2. “Authorization of remote access” should be deleted because in no way can you circumvent CIP-004-6 R4.1 requiring authorization of remote access to a high or medium impact BES Cyber System and there is no need to replicate that requirement again in this Standard. Additionally, CIP-005 R1.3 requires explicit access permissions and documented business justifications for all ‘system-to-system’ access, including vendor-initiated access. With respect to “logging and monitoring”, and the detection of “unauthorized activity”, we have serious concerns over the proposed language and provide that CIP-005-5 R1.5 already requires the detection of inbound and outbound malicious communications, CIP-007-6 R4 already requires the

logging and controlling of access at each ESP boundary and to BES Cyber Systems, and CIP-008-5 R2 already requires response to detected Cyber Security Incidents, which includes unauthorized activity during a vendor remote access session. As drafted, a failure to comply with R4 could place a Responsible Entity in possible double jeopardy with those other requirements. Additionally, as written, R4 creates a scope expansion of the existing CIP-005-5 R1.5 currently applicable to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers to now ropes in all Medium Impact BES Cyber Systems – leaving entities (and auditors) to determine "which Standard wins?"

Based on those concerns, Southern Company recommends the complete removal of R4 from the Standard, and where additional controls not already covered in an existing Standard are directed in the FERC Order, those controls should be covered under "the plan(s)" under R1 in a similar manner as the proposed edits provided under R1.

If R4 is not removed in this manner, we provide the below edits for consideration with the following comments. In addition to the justified removal of "authorization of remote access", logging and controlling are achievable concepts due to their requirement under existing Standards and therefore should not be required again here in this Standard and removed. This leaves "methods to disable remote access sessions", which we propose moving under the main R4 for the applicable scenarios. Again, detecting and responding to "unauthorized activity" is already required under existing Standards, and should be removed from R4. If not removed, the SDT must address the discrepancy between the scope collision between the draft R4 and CIP-005-5 R1.5.

Additionally, if there is an expectation beyond the use of IDS/IPS for "detecting unauthorized activity", then we would argue that it is nearly impossible for an entity to look at a stream of 1's and 0's flowing by at a several megabits per second and determine whether there is "unauthorized activity" or not in that stream. With the difficulty in determining "unauthorized activity" in a stream of bits flying by, we respectfully recommend striking this and request the SDT to consider focusing the controls in this requirement specifically to having methods to rapidly "disable remote access" to prevent remote control of entity assets.

Modify R4 language as follows:

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall address methods to disable remote access sessions for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s). [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]

Likes 0	

Dislikes 0	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT supports the IRC comments and offers the following supplemental comments.

Requirement R4 is duplicative of existing requirements in CIP-004, CIP-005, CIP-007, and CIP-008. The drafting team should consider modifications to these existing standards rather than creating new requirements in a new standard. By placing these requirements in a stand-alone Standard, there is a possibility that entities may not make necessary connections to the prerequisites of some requirements (e.g., CIP-004 R2, R3) and downstream obligations of other requirements (e.g., CIP-008). ERCOT offers the following suggestions for realignment:

Requirements for electronic access authorization of vendors, including Interactive Remote Access, are addressed within CIP-004 R4, which also addresses the proper vetting and training of said vendors. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper pre-authorization requirements.

Requirements for Interactive Remote Access are already addressed within CIP-005 R2. Vendor-initiated remote access is just one example of Interactive Remote Access. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper configuration of remote access (e.g. multi-factor authentication, encryption, Intermediate System).

Requirements for system-to-system communications are already addressed within CIP-005 R1. This requirement could be added to CIP-005 R1 or as an addition to R2. The heading for Table 2 within CIP-005 can be modified to “Remote Access” in support of this. If the SDT keeps the requirement in CIP-013, the requirement should be modified to address proper network controls for the system-to-system communication (e.g. ESPs, EAPs, etc.).

Requirements for logging and monitoring of access activity are addressed in CIP-007 R4. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify the logging specifications that differ from CIP-007 R4. Requirements for response to unauthorized activity are already addressed within CIP-008. If the SDT keeps the requirement in CIP-013, the requirement should be modified to identify integration with CIP-008. There are also several instances in the standard where language needs to be clarified. The drafting team should state whether system-to-system remote access includes "phone home" capabilities that are used for reporting of licensing, system health, and system problems. Requirement R4.1 should be clarified to specify whether it is addressing authorization of each remote access session or remote access to the vendor in whole. The drafting team should consider whether this requirement is consistent with current requirements in CIP-004 R4. The drafting team also needs to address authorization of software companies that use a "follow-the-sun" support model. Follow-the-sun is a type of global support where issues are passed around daily between work sites that are many time zones apart. Such a support increases responsiveness. As noted with other requirements in the draft CIP-013 standard, the drafting team should address situations in which vendors will not or cannot provide the levels of service mandated by this requirement. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling to agree. To address the concern, the drafting team should include a limited exemption from compliance, such as a Technical Feasibility Exception (TFE), which would protect Responsible Entities in the event a vendor is unwilling to agree to the terms otherwise required by R4. NERC's Appendix 4D to the Rules of Procedure provides for a basis of approval of a TFE beyond strict technical limitations of a system. (See Section 3.0 of the appendix.)	
Likes 0	
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements	
Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	
We are in general agreement with EEI comments on this requirement.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Scott Downey - Peak Reliability - 1	
Answer	No
Document Name	
Comment	

Access into the ESP is controlled for vendors the same as FTEs. That process is already outlined in other CIP requirements. If this is meant to be an alternative avenue of access outside the rest of the standards that is not clear.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
The standard should not create additional requirements for which entities are already being audited against. This creates confusion and risks the entity to being in double jeopardy for the same activity. NRECA recommends revising R4 to address the following: R4, Part 4.1 is already covered under CIP-004-6 R4, Part 4.1 R4, Part 4.2 is already covered under CIP-007-6 R4, Part 4.1 R4, P4.3 is already covered under with CIP-005-5	
Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	

Answer	No
Document Name	
Comment	
- See APPA's comments, with which SVP agrees.	
Likes 0	
Dislikes 0	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	

We have questions and concerns about how R4 would be applied. Please see the associated comments in Question 9.	
Likes 0	
Dislikes 0	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
This Requirement is duplicative of CIP-005-5.	
Likes 0	
Dislikes 0	

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	

Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 4.	
Likes 0	
Dislikes 0	

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes identifying and logging unauthorized access is already covered. In CIP-005. Furthermore, SunPower believes that 4.3, disabling the threat of unauthorized access to BES Cyber Systems should be addressed through a revision to CIP-007, where controls for external access are covered.	
Likes 0	
Dislikes 0	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
The NERC CIP Cyber Security Standards already have one of the most specific remote access security standard through CIP-005. Additional specifications to remote access should not be placed in a supply chain cyber security risk management Standard.	
Likes 0	
Dislikes 0	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend moving R4 into the following Standards/Requirements CIP-005 R2, CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 to address FERC order No. 829.

2) Recommend that this Rationale needs to be updated from “machine-to-machine” to “system-to-system” for consistency

3) The first sentence of R2 is broader than the second sentence. The first sentence is “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems.” The second sentence is “The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s):“ Recommend that the first sentence needs to be consistent with the Order and reference *vendor-initiated* remote access and not *vendor* remote access.

4) Request guidance. “Vendor-Initiated” could be considered a single word and not associated with the proposed definition of “vendor”.

5) Recommend changing R4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“ to “Disabling or otherwise responding to *detected* unauthorized activity.“

6) The phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected.

Consider eliminating sub requirements 4.1 and 4.2 since they are covered in CIP-005 and CIP-007, R5 respectively. Consider addressing sub requirement 4.3 by modifying CIP-005 thus eliminating R4 from the proposed CIP-013 standard.

R4 should be moved to CIP-005 since this requirement, as written in CIP-013, only applies to vendors having remote access. This does not address other sources of remote access threats as written.

For R4.2, we suggest limiting the retention period for evidence logs to 90 days to be consistent with CIP-007 R4, Parts 4.1, 4.2, and 4.3.

This would increase the scope of file integrity monitoring to Medium impact devices, some which are not capable of logging. This would discourage entities from allowing vendors to ever log in remotely, which might hinder reliability in the case of required emergency troubleshooting/support. Lack of timely support would also force entities to be non-compliant with other standards, such as other CIPs.

Remove vendor remote access from scope and only include system-to-system. Vendor remote access is already addressed in CIP-005 R2. SDT appears to be building on top of CIP-005 R1.5; however, R4.3 says “during the remote access session,” which may not reasonable amount of time since this is a real-time action.	
Likes 0	
Dislikes 0	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	

Control of Interactive Remote Access to High and Medium Impact BES Cyber Systems is already required by CIP-005-5, Requirement R2. To that end, including that aspect in this Requirement is duplicative to some extent. Similarly, it could be argued that authorization of remote access is covered by CIP-004-6, Requirement R4, and logging of access is required by CIP-007-6, Requirement R4. The Standards Drafting Team should either incorporate the few remaining elements into the existing Requirements in the other CIP Standards, or rewrite this Requirement to only include the additional expectations not covered elsewhere.

Likes 0	
Dislikes 0	

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC disagrees with the proposed requirement. CIP-013-1 R4 requires actions to be taken by the Responsible Entity that are outside of the supply chain context. FERC Order 829 specifically stated in paragraph 45 that the plan should address the security objectives in "the context of addressing supply chain management risks." NIST 800-53 provides a definition of supply chain that is as follows: "Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer." FERC Order 829 acknowledges this definition in paragraph 32, footnote 61. However, the SDT has chosen to identify controls in R4 that are executed only as part of the day-to-day management of BES Cyber Systems and introduce double jeopardy with existing CIP Reliability Standards.

R4 as written contains three parts to each be implemented for "(i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)."

4.1: Authorization of remote access. Electronic access to high and medium impact BES Cyber Systems, whether local or remote, and regardless of whether the individual is a vendor, is already required by CIP-004-6 R4, Part 4.1. System to system remote access must be explicitly permitted through the ESP along with documented justification according to CIP-005-5 R1, Part 1.3.

4.2: Logging and monitoring of remote access sessions: CIP-005-5 R1, Part 1.5 requires methods for detecting malicious communications for high impact BES Cyber Systems and medium impact BES Cyber Systems at Control Centers. CIP-007-6 R4, Part 4.1 requires logging of successful and failed access attempts. The applicable systems for CIP-007-6 R4, Part 4.1 includes EACMSs associated with medium and high impact BES Cyber Systems, effectively including logging that occurs at the perimeter of the ESP as well as access to the BES Cyber Systems directly. CIP-007-6 R4 additional requires monitoring of the logs.

4.3: Disabling or responding to unauthorized activity: CIP-008-5 R2 requires that entities respond to unauthorized activity according to their defined incident response plans. As a Cyber Security Incident includes any incident that "compromises, or was an attempt to compromise, the ESP…" or "disrupts, or was an attempt to disrupt, the operation of a BES Cyber System," response to any unauthorized activity (whether local or remote, physical or electronic) is already required by CIP-008-5 R2.

That said, there are gaps remaining between the existing CIP standards and the directive as specified by FERC Order 829.

As such, all controls required by CIP-013-1 R4 already exist in other CIP Reliability Standards, effectively making any non-compliance with R4 a case of double jeopardy with either CIP-004-6 R4, CIP-005-5 R1, CIP-007-6 R4, or CIP-008-5 R2, depending on the facts and circumstances of the specific compliance issue. While CIP-013-1 R4 suggests the implementation of technical security controls, it is unclear what additional controls would be implemented that are not already required by the existing CIP Standards. CIP-013-1 R4 only provides for additional paperwork, administrative burden, and double jeopardy compliance risk. As such, the standard drafting team should not create additional requirements for which entities are already being audited against and it should be removed.

That said, we do believe that addressing remote access in the supply chain context (not in the day-to-day operations context) could provide supply chain security risk management benefits. Unfortunately, the SDT has not constructed its requirement as such. Consistent with our response to question 1, we recommend that the SDT consider a plan based approach to addressing security risks in the context of the supply chain.

R4 is written in a manner that implies the Responsible Entity shall implement a separate documented process in addition to the plan specified in R1. Paragraph 45 of Order No. 829, clearly specifies this objective of vendor remote access should be applied to "The Plan" identified in the core directive in the context of addressing supply chain management risks. (P. 45) The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. GTC recommends the SDT remove this requirement and include a security objective for vendor remote access in "The Plan" specified in R1 to align with the FERC Order. See GTC's comment for Question #1.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
Authorization of Remote Access The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap. Activity v. Access The use of "activity" in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as "escorted cyber access." In almost all cases, the reason the Responsible Entity is	

allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If "activity" is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they'll be able to do it onsite. We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard "must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions." (Order No. 829, P51) The security objective is to address "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." (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated "Charles Angels" style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a "how" to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor's ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the "monitoring" language to "control" and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-

machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it's unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC

Answer	No
Document Name	
Comment	

The IRC and SWG request that the SDT consider moving this requirement to existing CIP Standard to prevent overlap, conflict, or omission of existing requirements.

The SDT should address whether system-to-system access is when vendor-initiated. Lack of clarity there will impact automated updates from vendors that are time-sensitive, as well as outbound connections to vendors for health checks, licensing, and other system information.

Likes 0	
Dislikes 0	

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF

Answer	No
Document Name	
Comment	

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is

allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the Responsible Entity would not be able to recognize inappropriate actions. If "activity" is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they'll be able to do it onsite. We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard "must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions." (Order No. 829, P51) The security objective is to address "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." (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated "Charles Angels" style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a "how" to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor's ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the "monitoring" language to "control" and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-

machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it's unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	
Comment	

This requirement is duplicative of existing requirements within CIP standards.

Authorization of access is covered in CIP-004-6 R4.1. The language in this CIP-004-6 R4.1 does not exclude vendors.

The rationale for CIP-007-6 R4 explicitly states that security event monitoring's purpose is to detect unauthorized activity.

A detection of unauthorized activity would be investigated as a potential Cyber Security Incident and appropriate action would be taken from there.

Likes 0	
Dislikes 0	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No
Document Name	
Comment	

SDG&E agrees with EEI comments and proposed language. These operations requirements are covered in other CIP standards.

Likes 0	
Dislikes 0	

Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

Authorization of Remote Access

The existing CIP-004 requirements already address authorization of vendor individuals and CIP-005 requirements address system-to-system authorization. We recommend that the SDT consider deleting Requirement R4, Part 4.1 to avoid this unnecessary overlap.

Activity v. Access

The use of “activity” in 4.2 and 4.3 is a concern because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. Also, there is no such thing as “escorted cyber access.” In almost all cases, the reason the Responsible Entity is allowing the remote vendor to support the system is that they have knowledge and skills that the Responsible Entity does not. Therefore the

Responsible Entity would not be able to recognize inappropriate actions. If "activity" is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they'll be able to do it onsite. We recommend that the SDT consider changing "activity" to "access" in parts 4.2 and 4.3.

Remote Access Session Monitoring

Although the Commission mentions monitoring of third-party initiated remote access sessions, they direct that the standard "must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions." (Order No. 829, P51) The security objective is to address "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." (Order No. 829, P 52).

First, the CIP-005 two factor authentication requirement would prevent access via stolen vendor credentials, except for in a sophisticated "Charlie's Angels" style attack (2000 movie) designed to overcome multifactor authentication, which was not the case in the Ukraine attack.

Second, monitoring remote access sessions to detect unauthorized activity is a method to control unwanted access or a "how" to implement the security objective. There are other methods to address the security objective, including controlled log-in and log-outs for specific activities and limiting the vendor's ability to access BES Cyber Systems.

Third, session monitoring of system to system activity, as prescribed by the proposed standard is not practical due to technology constraints and the likelihood that time sensitive network traffic supporting reliability tasks could be adversely impacted. For example, where a 2 millisecond response is required in an energy management system and continuous monitoring of remote vendor access reduces system response time to 5 milliseconds. Also, technology constraints may prevent Responsible Entities from determining whether a vendor or an employee is accessing the BES Cyber System. These complications may force Responsible Entities from disallowing remote access by vendors, which may actually harm reliability rather than improve it. Vendors know their systems best since they designed and manufactured them and therefore they are in the best position for remote access to complete certain tasks.

To address the concerns, we recommend that the SDT consider changing the "monitoring" language to "control" and focus on the second part of the security objective, controlling persistent machine-to-machine remote access sessions by vendors. Controlling persistent machine-to-

machine remote access is possible by different methods, including one way communications and time limiting access sessions. Vendor Interactive Remote Access is already controlled by CIP-005 requirements.

Disabling/Responding to Unauthorized Activity

Disabling remote access (Part 4.3) may also not be possible and would likely force Responsible Entities to disallow vendor remote access. We recommend that the SDT remove this part.

Requirement Placement (CIP-005)

Because Requirement R4 is an operational control, we recommend that the SDT consider putting this requirement into CIP-005 R2 and not create duplicative requirements.

Definitions

Machine-to-machine or system-to-system remote access is also not defined so it's unclear what new systems this brings into scope for this requirement. If the SDT uses one of these terms, we recommend that they define it. Also, if the SDT uses our suggestion for addressing persistent, machine-to-machine remote access, we also recommend defining persistent, perhaps leveraging the concept used by the transient cyber asset definition. We also recommend that the SDT consider defining vendor, for example, does it include an ISO ICCP connection to an EMS?

We recommend the following language for consideration by the SDT:

R4. Each Responsible Entity shall implement one or more documented method(s) to control persistent, machine-to-machine remote access sessions by vendors to high and medium impact BES Cyber Systems.

Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
SMUD requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access. Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. SMUD requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. SMUD requests changing the language to “upon detected unauthorized activity”.	
Likes 0	
Dislikes 0	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	

The NYPA Comments	
Likes 0	
Dislikes 0	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	

Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	

FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx
Comment	

The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.

Seattle City Light requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Seattle City Light requests that the scope of R4 be limited to disabling remote access.

For R4.3, the phrase “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Seattle City Light requests changing the language to “upon detected unauthorized activity”.

Furthermore, because it may not be technically feasible to remotely disable a vendor from equipment provided by that vendor (which the entity purchased from them, and may be dependent upon the vendor for maintenance), Seattle City Light requests the inclusion of a Technical Feasibility Exception (TFE) for R4. Seattle City Light suggests the following language: "WHERE TECHNICALLY FEASIBLE, each responsible entity shall implement one or more documented process(es) for controlling vendor remote access to…" (emphasis added).	
Likes 0	
Dislikes 0	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO request that the SDT consider moving this requirement to existing CIP Standard to prevent overlap, conflict, or omission of existing requirements. The SDT should address whether system-to-system access is when vendor-initiated. Lack of clarity there will impact automated updates from vendors that are time-sensitive, as well as outbound connections to vendors for health checks, licensing, and other system information.	
Likes 0	
Dislikes 0	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No

Document Name	
Comment	
Colorado Springs Utilities (CSU) requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access. Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. CSU requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. CSU requests changing the language to "upon detected unauthorized activity".	
Likes 0	
Dislikes 0	
Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	
See EEI comments	
Likes 0	
Dislikes 0	

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) R4 creates confusion and possible double jeopardy with other standards. Recommend modifying modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 address the FERC order No. 829.

2) For R4.3, the “during remote access” does not seem to align with the “timely manners” guidance given on page 15, line 23 of the Guidance and Examples document. This capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. Suggest changing to “detected unauthorized activity”.

3) Suggest changing the format of the standard to use Applicability Tables like those used in CIP-004 through CIP-011.

Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA believes the scope should be limited to High and Medium BES cyber systems with ERC or dialup. All requirements for Low impact systems should be addressed in CIP-003. BPA suggests modification of existing CIP standards to address gaps: Remote access CIP-013 R4, P4.1 is addressed in CIP-004-6 R4, Part 4.1 Logging and monitoring CIP-013 R4, P4.2 is addressed in CIP-007-6 R4, P4.1 Remote access sessions CIP-013 R4, P4.3 is addressed in CIP-005 R2	
Likes 0	
Dislikes 0	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	

Comment
This requirement is duplicative of existing requirements within CIP standards. Authorization of access is covered in CIP-004-6 R4.1. The language in this CIP-004-6 R4.1 does not exclude vendors. The rationale for CIP-007-6 R4 explicitly states that security event monitoring's purpose is to detect unauthorized activity. A detection of unauthorized activity would be investigated as a potential Cyber Security Incident and appropriate action would be taken from there.

Likes 0	
Dislikes 0	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	

Comment
Santee Cooper requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access. Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP electronic access requirements. Santee Cooper requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and

would be dependent on how the unauthorized activity was detected. Santee Cooper requests changing the language to “upon detected unauthorized activity”.	
Likes 0	
Dislikes 0	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Rationale for Requirement R4:

The rationale language for R4 states, “The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51).” R1, R2, and the Rationale for Requirement R3 and R4 do not specify the impact classifications (High, Medium and Low) when referencing the BES Cyber System. R3 and R4 specifically state the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems (R3)” or “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems (R4).” IPC would like to know if the inconsistent impact classification references were intended or were an oversight by the SDT?

R4

IPC does not believe CIP-013-1 is an appropriate standard to address R4.1, R4.2 and R4.3. IPC believes R4.1 belongs in CIP-004-6, as R4.1 is related to authorization and R4.2 and R4.3 belongs in CIP-005-6 as R4.2 and R4.2 are related to remote access. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-004-6 addresses access management and CIP-005-6 addresses remote access.

M4 Some of the measure language for R4 states, “hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.“ R1, R2, and the Rationale for Requirement R3, R4, and M4 do not specify the impact classifications (High, Medium and Low) when referencing the BES Cyber System. R3 and R4 specifically states the impact classification of the BES Cyber System “applicable to High and Medium Impact BES Cyber Systems (R3)” or “Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems (R4).” IPC would like to know if the inconsistent impact classification references were intended or were an oversight by the SDT?	
Likes 0	
Dislikes 0	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016. Reclamation recommends that Requirement R4 be deleted. There would be no need for Requirement R4 if all aspects of the supply chain risk management plan(s) are to be addressed in Requirement R1 and its sub-requirements.	
Likes 0	
Dislikes 0	

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	
1. As mentioned above, the standard drafting team should not create additional requirements for which entities are already being audited against. This creates confusion and risks the entity to being in double jeopardy for the same activity. R4, Part 4.1 is covered under CIP-004-6 R4, Part 4.1 R4, Part 4.2 is covered under CIP-007-6 R4, Part 4.1 R4, P4.3 is covered under with CIP-005-5. Part 1.3 of CIP-005-5	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	

Dislikes 0	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
Requirement R4: ATC agrees with the value provided through the implementation of controls to address logging and controlling third-party initiated remote access; however, ATC has voted “No” to the proposed language developed CIP-013-1 Requirement R4 because existing Reliability Standards accomplish this objective rendering the need for this requirement in CIP-013-1 moot. In its redundancy, it is at odds with the former efforts	

associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

Requirement R4 Sub Requirement 4.1 – 4.3:

CIP-013-1 R4 is simultaneously duplicative and additive to the language and/or intent of several existing approved and effective CIP Cyber Security Reliability Standards and is therefore providing no additional security or reliability value and creating a condition of double jeopardy for Registered Entities where a violation of CIP-013-1 R4 would constitute a violation of another CIP Standard and requirement.

CIP-004-6 R4 and R5 address access management and revocation for individuals having cyber access to specified high and/or medium impact-rated BES Cyber Systems and associated Cyber Assets. The existing enforceable CIP-004-6 standard is silent to the capacity with which a given individual is engaged with a Registered Entity, and therefore in its silence it addresses employees, contractors, interns, apprentices, or even vendors etc. These access requirements within CIP-004-6 are more prescriptive than what is proposed for CIP-013-1 therefore providing no additional security or reliability value and ultimately rendering CIP-013-1 R4.1 superfluous and unnecessary.

CIP-005-5 R1 Parts 1.1 – 1.4 addresses CIP-013-1 R4(i), R4.1, ultimately rendering CIP-013-1 R4(i), R4.1 superfluous and unnecessary in that:

o CIP-005-5 R1 Parts 1.3 mandates authorization for system-to-system remote access through the requirement for inbound and outbound access permissions through an identified Electronic Access Point protecting high and/or medium impact-rated BES Cyber Systems,

where those BES Cyber Systems must already be protected as a function of being inside an identified Electronic Security Perimeter pursuant to CIP-005-5 Requirement R1 Part 1.1, and

where all External Routable Connectivity must be through an identified Electronic Access Point pursuant to CIP-005-5 Requirement R1 Part 1.2.

o Additionally, CIP-005-5 R1 Part 1.4 obligates Registered Entities to perform authentication for establishing Dial-up connections to high and/or medium impact-rated BES Cyber Systems, where technically feasible. The broad reference to system-to system remote access (which is silent to Dial-up) in combination with the absence of the provision for technical feasibility within this draft Requirement is effectively and expansion in scope to the already approved and enforceable CIP-005-5 R1 Part 1.4 Reliability Standard. Any expansion in scope to remote access requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-005-5 so as not to be

effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-005-5 R1 Part 1.4 through a CIP Senior Manager and regional regulator approved Technical Feasibility Exception becomes a matter of non-compliance pursuant to CIP-013-1 R4.

CIP-005-5 R2 Parts 2.1 – 2.3 and CIP-007-6 R5 Parts 5.1 goes beyond in addressing CIP-013-1 R4(ii), R4.1, ultimately rendering CIP-013-1 R4(ii), R4.1 superfluous and unnecessary in that:

o CIP-005-5 R1 Parts 2.1 mandates authorization for all Interactive Remote Access (IRA) (including vendor-initiated IRA) through the requirement to use an Intermediate System such that any remotely-initiated IRA does not directly access the high and/or medium impact-rated BES Cyber System(s),

o where those Intermediate System must also utilize encryption that terminates at the Intermediate System pursuant to CIP-005-5 Requirement R2 Part 2.2, and

o where all IRA sessions must require multi-factor authentication pursuant to CIP-005-5 Requirement R2 Part 2.2.

o CIP-007-6 R5 Parts 5.1 further mandates methods to enforce authentication of interactive user access (including vendor-initiated users) where technically feasible for high and/or medium impact-rated BES Cyber System(s),

CIP-005-5 R1 Parts 1.2 - 1.5, in combination with CIP-007-6 R4 Parts 4.1-4.4 and CIP-007-6 R5 Part 5.7 collectively addresses, and in some cases exceeds, the logging, monitoring, and detection of unauthorized activity proposed in CIP-013-1 R4, R4.2, ultimately rendering in CIP-013-1 R4, R4.2 superfluous and unnecessary in that:

o CIP-005-5 R1 Part 1.5 mandates one or more methods for detecting known or suspected malicious communications both inbound and outbound on the Electronic Access Points protecting high and/or medium impact-rated BES Cyber System(s), and because all remote access must also be through an identified Electronic Access Point pursuant to CIP-005-5 Requirement R1 Part 1.2, the two existing enforceable requirements in combination already satisfying the detection component intended by CIP-013-1 R4, R4.2; and consequently, the detection component intended by CIP-013-1 R4, R4.2 adds no security or reliability value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-005-05 R1.

o CIP-007-6 R4 Parts 4.1-4.4 mandates that, per BES Cyber System capability or at the Cyber Asset level for high and/or medium impact-rated BES Cyber System(s),

specified access-related events are logged,

alerts are generated for said events,

event logs are retained as technically feasible for 90 consecutive calendar days except in CIP Exceptional Circumstances,

thereby already satisfying the logging and monitoring component intended by CIP-013-1 R4, R4.2; Consequently, the logging and monitoring component intended by CIP-013-1 R4, R4.2 adds no security or reliability value and rather creates a condition of potential double jeopardy for existing approved and enforceable Standard CIP-007-6 R4 that is also at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

Furthermore, in its redundancy of CIP-007-6 R4, CIP-013-1 R4, R4.2 is simultaneously an expansion in scope in that CIP-013-1 R4, R4.2 is silent to the provisions for “Per Cyber System capability”, per cyber Asset capability”, “technical feasibility”, and “CIP Exceptional Circumstances”, is effectively and expansion in scope to the already approved and enforceable CIP-007-6 R4 Reliability Standard. Any expansion in scope to logging, monitoring, or detection activity related to requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-007-6 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-007-6 R4 through:

- a CIP Senior Manager and regional regulator approved Technical Feasibility Exception,
- a CIP Senior Manager approved CIP Exceptional Circumstance,
- a documented per BES Cyber System incapability, and/or
- a documented per Cyber Asset incapability

becomes a matter of non-compliance pursuant to CIP-013-1 R4.2

o CIP-007-6 R5 Part 5.7 mandates limiting of the number of unsuccessful authentication attempts or the generation of alerts of unsuccessful authentication attempts exceeding a Registered Entity defined threshold, where technically feasible and scope to high impact BES Cyber Systems and medium impact BES Cyber Systems at Controls Centers. The broad reference high and medium impact BES Cyber Systems, in combination with the absence of the provision for technical feasibility within this draft Requirement for CIP-013-1 R4 is effectively and expansion in scope to the already approved and enforceable CIP-007-6 R5.7 Reliability Standard. Any expansion in scope to logging, monitoring, or detection activity related to requirements or controls for high or medium impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes for CIP-007-6 so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one. Furthermore, it is a contradiction between standards where compliance with one requirement in CIP-007-6 R5 Part 5.7 through a CIP Senior Manager and regional regulator approved Technical Feasibility Exception becomes a matter of non-compliance pursuant to CIP-013-1 R4.

Likes 0	
Dislikes 0	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	

OUC requests that the scope of R4 be limited to high and medium BES Cyber Systems with ERC or Dial-up Connectivity as these systems have the highest risk associated with remote access.

Elements of R4 (authorization, logging/monitoring) appear duplicative of existing CIP requirements. OUC requests that the scope of R4 be limited to disabling remote access. For R4.3, the phrase "during remote access" does not seem to align with the "timely manners" guidance given on page 15, line 23 of the Technical Guidance and Examples document. The capability to disable during the remote access session may not always be possible and would be dependent on how the unauthorized activity was detected. OUC requests changing the language to "upon detected unauthorized activity".	
Likes 0	
Dislikes 0	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes
Document Name	

Comment

The Technical Guidance and Examples state that "for Requirement R4 Part 4.1, an entity may already have some authorization controls in place that will support meeting this objective", including CIP-004 and CIP-007 R5 controls if they are fully implemented for vendor-initiated Interactive Remote Access. Please confirm that implementation of these controls for all remote access, vendor or entity initiated, would meet compliance with this requirement. If so, would it be beneficial to caveat the requirement and have it read "**4.1** Authorization of remote access, not previously approved by CIP-004, by the Responsible Entity?"

A responsible entity may have numerous contractors from various vendors that perform a number of tasks within CIP environments that are on-site, sitting right next to employees engaged in similar activities. Both the contractors and the employees normal work process may have them utilize Interactive Remote Access to perform their responsibilities efficiently. Are these contractors, embedded and onsite, to have each of their connections explicitly approved and monitored at a different level of scrutiny than actual employees of the responsible entity, simply because they are not employees? Or will there be a distinction between on-site and off-site "vendors?"

Likes 0	
Dislikes 0	

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	Yes
Document Name	
Comment	
R4 could give entities the impression that they do not need to follow the CIP-005-5 R2 controls for Interactive Remote Access. If an entity did not leverage its existing Interactive Remote Access (CIP-005-5 R2) processes to support this Requirement, WECC is concerned that separate vendor remote access processes may provide additional ingress/egress points into the ESP. An entity should ensure that vendor remote processes are protected at least to the level of CIP-005-5 R2. At no point in time, should there ever be an unmonitored connection into a BCS. This is something that is totally under the control of the entity. Even if the vendor includes a "phone-home" feature on a system or application, the ingress and egress of that connection should still be monitored and controlled by the entity to minimize the risk of third-party penetration into the BCS. The SCRM team should work closely with the CIP-005-5 team to ensure all remote access connections are managed, monitored, and controlled through an Electronic Access Control and Monitoring System [EACMS] and/or Intermediate System [IS]	
Likes 0	
Dislikes 0	

Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
While in overall agreement with this Requirement R4, ACEC would recommend the following change: 1. Move Requirement 1, Part 1.2.2, "Process(es) for notification when vendor employee remote or onsite access should no longer be granted" and Part 1.2.6 "Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)" to Requirement R4 since this requirement is where Vendor Remote Access is addressed.	

Likes 0	
Dislikes 0	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
This appears to meet the FERC directive.	
Likes 0	
Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	Yes
Document Name	
Comment	
We recommend the SDT address CIP Exceptional Circumstance with respect to this requirement aligned with project 2016-02. Also please see our earlier comments with regards to redundancy between R4 and R1.2.6.	
Likes 0	
Dislikes 0	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • Recommend changing Requirement 4.3, from "Disabling or otherwise responding to unauthorized activity during remote access sessions" to "Disabling or otherwise responding to detected unauthorized activity associated with remote access sessions." PSEG finds that inclusion of the word "during" in the requirement overreaches the intent of relevant FERC directive (p.51).	

- Requirements R1 and R2 do not require the registered entity to go back and revise previous contracts. In order to comply with this requirement, R4, past contracts / vendor service agreements may be required. Alignment is needed between R1, R2, and R4.

- Vendor-initiated Interactive remote access is no different than Interactive remote access. Recommendation to incorporate Requirement R4 into CIP-007 R5 System Access Control.

- Requirement R4 overlaps with CIP-005 for Interactive Remote Access, which applies to vendors, only 4.2 monitoring and 4.3 is new. Recommend streamlining R4 to fit in CIP-005 R2.

- Recommend changing “activity” to “access”. Use of the word “activity” in 4.2 and 4.3 because it may be difficult for a Responsible Entity to determine whether the activity is authorized or unauthorized. In almost all cases, the vendor has more in depth technical knowledge of the system they developed beyond the Registered Entity’s level of expertise on the system. Therefore it would be difficult for the Responsible Entity to recognize inappropriate actions/activity. If “activity” is left, this will likely result in Responsible Entities requiring vendors to perform their work onsite, which will add considerable costs without any security benefits. If the person is doing something inappropriate, they’ll be able to do it onsite. If the intent of this requirement is to monitor “unauthorized activity”, the term “unauthorized activity” should be defined.

Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Stephanie Little - APS - Arizona Public Service Co. - 5

Answer	Yes
Document Name	

Comment

AZPS requests changing Requirement R4.3 to read ‘disabling or otherwise responding to **detected,** unauthorized activity during remote access session’. It further notes that, as written, the proposed Requirement R4 would place Registered Entities in “double jeopardy” where similar

controls are already required under CIP-004-6. Accordingly, AZPS requests that the SDT consider revising this requirement to remove such redundancy or to include a clarification regarding how this risk for "double jeopardy" will be managed relative to access controls required under CIP-004-6.	
Likes 0	
Dislikes 0	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	
Document Name	
Comment	
N/A	
Likes 0	

Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	

5. The SDT developed CIP-013-1 Requirement R5 to address Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems (P 48 and P 51). Do you agree with the proposed requirement? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement provide your recommendation and explanation.

Summary Consideration. The SDT thanks all commenters. The SDT has removed low impact BES Cyber Systems from applicability of CIP-013-1 and is not proposing any new requirements to address cyber security supply chain risks for these cyber systems. The SDT believes that the CIP-013-1 proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829.

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	No
Document Name	
Comment	

The NSRF does not understand the intent of the following:

R1 is applicable to “Each Responsible Entity” is to implement “one or more supply chain risk management plans”.

R2 is applicable to “Each Responsible Entity” is to review and update its “supply chain risk management plans” at least once every 15 calendar months.

R5 is applicable to “Each Responsible Entity” with at least one “low impact BES Cyber System” will have a documented “cyber security policies “ which require “review and approval” at least once every 15 calendar months.

For R5.1, imposes a requirement at the BES Cyber Asset level rather than at the BES Cyber System level. Consider removing R5.1 or reworking so it is applicable at the BES Cyber System level.

The NSRF has concerns with R5. As written, every entity with a "low impact BES Cyber System" is required to have "cyber security policies" (note policies should be changed to "policy(s)). This would include entities that have High and Medium impact BES Cyber Systems, as long as they have one "low impact BES Cyber System", too. Plus, R5.1 is a duplicate of R3 and R5.2 is a duplicate of R1.2.6.

This will cause double jeopardy for Each Responsible Entity in R1, R2, and R5. The "Responsible Entities" statement within each Requirement contains "High, Medium, and Low BES Cyber Systems". So everywhere "Responsible Entity" is used in the Standard, that requirement applies to everyone with High, Medium, and Low BES Cyber Systems.

The NSRF believes that this is NOT the intent of R5. If the intent of R5 is to have control for Entities with "low impact BES Cyber Systems" **only** then, it should be clearly stated. Such as:

*"R5. Each Responsible Entity with at least one asset identified in CIP-002, containing low impact BES Cyber Systems **only,** shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:"*

Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric

Answer	No
Document Name	

Comment

Requirement 5.1 needs to be removed. Currently patching is not required as a function for low impact assets. Until vulnerability and patching is made a requirement for low impact assets, then it is not possible to ensure that "all" patches for low impact assets be validated for authenticity. Additionally, given the issues with trying to validate authenticity for software and patches in general (see our comments on R3)

then this sub-requirement cannot be enforced. The sub-requirement for remote access is valid and should be implemented for low impact assets.	
Likes 0	
Dislikes 0	
faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

R5 requires a Policy for Low Impact BES Cyber Systems. The two sub requirements are more plan based than policy based and would recommend making them an addition to CIP-003-7(i) attachment A instead. This will keep all LOW Impact BES Cyber Asset requirements in one location.	
Likes 0	
Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
R5 fundamentally does not work as a low-impact scale-back of R3 and R4, because it can be meaningfully implemented only on a Cyber Asset level, and CIP-002-5.1 (R1.1.3) and CIP-003-6 (R2) do not require identification of Cyber Assets for low-impact BES Cyber Systems. The entire concept of R5 needs revision. The difference between supply chain risk management policies, as called-for in R5, and processes, mandated in R3 and R4, is unclear. TFE opportunity is again needed, nor should there be any obligation to impose measures on vendors (see our “additional comments” responses).	
Likes 0	
Dislikes 0	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
AEP is concerned about low impact BES Cyber Systems being included here because it may incentivize a lack of action on those systems in order to avoid compliance obligations. AEP believes the Standard should be reasonable for all to achieve, and this may create a significant recordkeeping burden for low impact systems. R5, as proposed, only requires a “documented policy”. Responsible entities could manage the risk appropriately for their circumstances without a requirement to “implement”.	
Likes 0	
Dislikes 0	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	

Answer	No
Document Name	
Comment	

See comments to Question 1.

These should clearly be modifications to CIP-003-7(i) Attachment A, and not lumped into CIP-013, Supply Chain Risk Management.

Likes 2	Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen; Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	No
Document Name	
Comment	

These risks should be evaluated during the procurement and deployment of vendor products and services (CIP-013-1 R1), and mitigated as part of the CIP-005 R2 and CIP-007 R2.

IID does not agree with including Low Impact BES Cyber Systems in this standard as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. As written, this requirement will place additional administrative burden on entities and the impacts are not fully understood. The SDT would need to clarify measures that would serve as evidence. As mentioned above, if the SDT feels that gaps remain, SRP feels that the modifications should be made in the standard where the topic is already addressed (CIP-003).

Additionally, IID feels that there should be exclusion comparable to a CIP Exceptional Circumstance (or TFE) added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.	
Likes 0	
Dislikes 0	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The current CIP requirements for BCS at low impact sites do not require identification of patch sources, or other patching procedural controls. Introducing R5 inadvertently requires utilities to develop a CIP-007 R2 program for low sites as well to be able to address software integrity. This policy would also require a software list and inventory of systems to provide evidence that the policy has been followed. Implementing CIP-013 essentially applies controls from CIP-005, CIP-007, CIP-008, and CIP-010 to BCS at low impact sites where there are no corresponding requirements within the existing CIP standards. For example, it is incongruous to require verification of patches on a low BCS for which there is no requirement to patch.	
Likes 0	
Dislikes 0	
Eric Ruskamp - Lincoln Electric System - 6	
Answer	No

Document Name	
Comment	
Smaller generation facilities are heavily dependent on the Original Equipment Manufacturers, and do not have the leverage to promote participation from large sole sources. How do facilities develop processes to verify integrity and authenticity of software and firmware, when OEMs don't offer guidance on validation? The sole sources also do not have the incentive to adhere to the same level of compliance when these assets are in their care, such as when embedded cyber assets are shipped off site to the OEM, or when service engineers are on site for commissioning. Enhanced compliance requirements discourages equipment servicing from the owner, and places more reliance on the OEM.	
Likes 0	
Dislikes 0	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy recommends the deletion of this requirement. As stated in our comments earlier, based on the minimal threat to stability that Low Impact BES Cyber Systems pose to the BES, coupled with the lack of an inventory list for said Low Impact systems to demonstrate compliance, we feel that this requirement is unnecessary and impossible to effectively demonstrate compliance to.	
Likes 0	
Dislikes 0	

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Requirement R5 speaks to documenting a policy or policies to address 5.1 and 5.2 for low impact BCS. The word “implement” is not in this requirement. Absent including the implementation piece, there is no requirement to implement the controls just document them. Furthermore, the SDT made it clear in Requirement R3 and R4 that an entity shall implement one or more documented process(es) for the actual security controls or processes. Similar language (implement documented process(es)) should be included in R5 versus policy. Even though the rationale section speaks to policies and processes, the language of the requirement only speaks to policies. This will drive consistent implementation across all BCS impact levels. ReliabilityFirst offers the following modifications for consideration to address our concern: R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall [implement] have one or more documented cyber security policies [or processes], which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:	
Likes 0	
Dislikes 0	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	

We request consistency in the use of terms between R1 and R5; R1 uses the term “plan” and R5 uses the term “process” or “policy”. We understand the term “plan” to mean a more high-level document that communicates management goals and objectives. We request clarification that the use of the term “policy” in R5 is meant to be a similar concept, i.e., that R5 is satisfied by a document that is reviewed and approved by the CIP Senior Manager that is a high-level document that communicates management goals and objectives, rather than a detailed process document with instructions to achieve the requirements. We seek this clarification because in the Technical Guidance and Examples (page 16 lines 29-31), the SDT writes “or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber System.” As described previously by the Version 5 SDT, a documented process and a policy are two different documents: a policy is a document used to communicate management goals and objectives, while a process is a set of required instructions specific to achieving the requirement. Based on the SDT’s comments in the Technical Guidance and Examples, it is unclear which will satisfy R5 and how it will be audited.

Clarification is also requested on whether “system to system” access applies to access that is “one-way” where the remote end conducts only monitoring activity and no control is possible. Can the procedure for access make distinctions for each methods of monitoring each type of access, Interactive Remote, system to system with control and system to system for monitoring only?

Additionally, we request confirmation that if vendors refuse or can’t provide hashes or other verification methods, an internal process to test, scan and perform verification activities be enough to satisfy requirement R5.1.

Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	

See NPCC Comments.	
Likes 0	
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	

AECI has concerns that R5, as written, would place Responsible Entities that have a combination of High, Medium, and low impact BES Cyber Systems at risk of double jeopardy. Part 5.1 is a duplicate of R3 and R5.2 is a duplicate of R1.2.6. This requirement should be removed from CIP-013-1 and addressed in CIP-003, R2, Attachment 1.	
Likes 0	
Dislikes 0	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	

PRPA is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. PRPA requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, PRPA requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	

AE is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. AE requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, AE requests that all requirements related to low impact assets be included in CIP-003.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003.

R5.1 is not consistent with R1.2.5, should R5.1 include the term “that are intended for use” to read “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and”

Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls R5 needs to be a process not a policy. If this is a policy, then suggest removing “controlling”

There should be exclusion comparable to a CIP Exceptional Circumstance added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable.

If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy. R5 should be a plan document and not a policy document.

Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT's intent?	
Likes 0	
Dislikes 0	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

CIP-013-1 R5 should be placed within CIP-003 in order to keep consistency with the approach used in the remaining CIP standards. Low impact requirements were placed in CIP-003 in order to keep all requirements within a single standard and requirement. By adding these requirements into a new standard, there is confusion resulting in an increased likelihood of a violation.

Guidance language should be added for the auditing process within the standard's guidelines and technical basis (not in a separate document). Not including this in the standard places no obligation on the auditors. Without this guidance language, the auditors could choose to audit in a near zero defect manner, as opposed to a quality of program manner. Providing clear guidance sets expectations for the entities.

Likes 0	
Dislikes 0	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters

Answer	No
Document Name	

Comment

We agree with the LPPC/APPA comments.

Likes 0	
Dislikes 0	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No

Document Name	
Comment	
CHPD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CHPD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CHPD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. SRP requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, SRP requests that all requirements related to low impact assets be included in CIP-003.	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No

Document Name	
Comment	
• This Requirement should be removed from the Standard. For consistency with the other CIP Standards (e.g. compare to the current draft revision of CIP-003-7i standard where Transient Cyber Asset language for assets that contain Low Impact BCS is included) applicability of supply chain risk management to assets that contain Low Impact BCS should be consigned to CIP-003, R1.2 and R2: o R2 – Attachment 1 should be expanded to include a Section for supply chain risk management (to include controls on software authenticity for Low Impact BCS, controlling vendor remote access to Low Impact BCS) o R1.2 – should be expanded to include supply chain risk management plan(s) with controls for assets that contain Low Impact BCS • The NERC Glossary of Terms definition of CIP Senior Manager will require update to include CIP-013	
Likes 0	
Dislikes 0	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Please refer to RSC- NPCC comments	
Likes 0	
Dislikes 0	

Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	No
Document Name	
Comment	
Basin Electric would prefer low impact requirements be included in CIP-003 rather than CIP-013. For R5.1, imposes a requirement at the BES Cyber Asset level rather than at the BES Cyber System level. Consider removing R5.1 or reworking so it is applicable at the BES Cyber System level. Basin Electric is concerned R5.1 will necessitate maintaining a list of low BES Cyber Systems and possibly a list of low BES Cyber Assets. Basin Electric suggests modifying the requirement to include clarification of when the obligation starts. Perhaps add language to the front of R5 such as: "For assets containing low impact BES Cyber Systems in production…"	

Likes 0	
Dislikes 0	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	
Comment	

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1. R5 will be the only low impact specific requirement not to be in CIP-003.

Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

Does R5 allow the Entity to “accept the risk?”

R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

Language of R5 should say "…shall document and implement one or more cyber security policies…" to clarify that implementation is expected for compliance. Draft R5 language does not include the term "implement".	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See comments on Requirement R5 in attached file.	
Likes 0	

Dislikes 0	

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment
N&ST believes it is inappropriate to try to define what amount to electronic access control requirements (vendor remote access) while revised electronic access control requirements in CIP-003 have not yet been formally approved.

Likes 0	
Dislikes 0	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment
As we reviewed Requirement R3 and Requirement R4, it is our understanding that a Management Plan needs to be developed and maintained. However, Requirement R5 is requiring security policies. At this point, we feel that there are inconsistencies in the Requirement language as well as potential Compliance Enforcement issues in reference to those particular Requirements. We would ask the drafting team to provide clarity on why Requirement R3 and Requirement R4 mentions Management Plans and Requirement R5 mentions security policies.

Additionally, the proposed language in Requirement R3 and Requirement R4 mentions high and medium Impact BES Cyber Systems. Requirement R5 mentions Low Impact BES Cyber Systems. Again, we would ask for clarity on why all three (3) Cyber Systems type aren't included in Requirement R3 through Requirement R5?

Finally, we suggest revising Requirement R5 language and moving it to the CIP-003 Standard. In the case that the drafting team doesn't agree with the revising of the Requirement's language, Our group recommends that this Requirement language be moved to the CIP-003 Standard because, we feel that it's the most appropriate Standard to handle this Requirement which is applicable to Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins

Answer	No
Document Name	

Comment

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5 Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.	
Likes 0	
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon has the same concerns regarding the lack of a compliance “safety valve”, the potential for double jeopardy as well as the administrative burden of updating the supply chain cyber security risk management plan(s) for newly identified vulnerabilities as included in the comments on R1-R4. The discussion under (4) identifies how the proposed R5 overlaps with existing CIP Standards.	
Likes 0	
Dislikes 0	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	

Vectren proposes that the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	No
Document Name	

Comment
We agree with EEI's recommendation to delete R5. Part 5.2 is duplicative with CIP-003-7, Attachment 1, Sections 2 and 3. Extending the operational controls for authenticity/integrity in Part 5.1 to low impact BES Cyber Systems is not commensurate with the risk. If the SDT thinks the risk to low impact BES Cyber Systems is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing the massive scope of these low impact systems. NERC's Compliance Registry Summary of Unique Entities and Functions as of March 3, 2017, identifies 1,398 unique NERC entities. These entities range from entities with a couple breakers for low impact Facilities (lines), to entities operating gigawatts of low impact generation units to entities operating high-impact Control Centers for thousands of miles of medium impact Transmission Facilities, for example. All have BES Cyber Assets, but very different risks.

Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	

Comment
We propose the SDT modify standard language based on Vectren's proposed language below: **R 5.**

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	No
Document Name	

Comment

- Dominion is of the opinion that all CIP policy requirements should be located in CIP-003 and that all requirements for low impact BES cyber assets should be placed in Attachment 1 of CIP-003. Placing all of the low risk operational CIP requirements in a single standard allows entities that have only low impact cyber assets to reference a single source for pertinent requirements.

- Dominion recommends the following modification to Part 5.1:

5.1: Verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to authorized installation into a low impact BES Cyber System."

- Dominion recommends the removal of Part 5.2. Access control obligations, including system-to-system remote access already exist in Section 3 of Attachments 1 and 2 of CIP-003-7 for low impact. CIP-003-7 is currently pending FERC approval.

Likes 0	
Dislikes 0	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	No
Document Name	

Comment

With the applicability of low impact BES Cyber Systems, this appears to negate a comment in CIP-002, R1.3 where it states, "… (a discrete list of low impact BES Cyber Systems is not required)".

What is the timing of R5.1 in terms of new software and existing software? The rationale explains that this starts in the operate/maintain phase of the life cycle but does the timing/life cycle language need to be added to the Standard rather than explained in the rationale section, which may not appear in the final language? Does this apply only to devices in production? For example, what if software is pre-loaded by an OEM. Is there an expectation that the Regional Entities work with their OEM to verify integrity and authenticity prior to this pre-loading? We seek more clarity in the language of R5 and recommend adding "…for Cyber Assets in production."

Regarding the security controls for vendor initiated and system-to-system remote access, R5 is about one or more documented policies and R4 is about the processes for authorization, logging and monitoring, and de-provisioning of remote access. With the requirement of one or more

documented cyber security policy, how would Responsible Entities enforce the policy(ies) without also requiring documented plan(s) and process(es), which R5 does not address?

There is no need to have R5 because coverage of low impact BCS is already included in R1. There are two options for R5: integrate it into either (1) existing applicable NERC CIP Standards or (2) R2, R3, and R4 of CIP-013-1.

For option #2:

R2 is about the periodic review and approval of the supply chain cyber security plan(s) developed in R1. R3 obligates Entities to define process(es) to verify the baseline components and any upgrades prior to BCS installation. Requirement R5.1 appears to be identical to R3 because the term "software" in R5.1 is broad in scope and includes the OS and commercially available or open source software.

If Entities are concerned with R4.2 for low impact BCS, the integration of R5 and R4 can either include (1) "per Cyber Asset capability" or "if technically feasible" language for low impact devices or (2) specific language of a risk-based approach, vendor or system, in determining where remote access controls will be applied.

We recommend option #1, the removal of R5 from CIP-013-1 and integration of the requirement into existing applicable NERC CIP Standards.

Likes 0	
Dislikes 0	

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

R5 discusses a Low policy – NRG recommends that this requirement should be moved to the CIP-003-7i standard where all CIP policy requirements are outlined.

As we reviewed the Requirements applicable to Requirement R3 and Requirement R4, it is to our understanding that a Management Plan needs to be developed and maintained. However, Requirement R5 is requiring security policies. At this point, we feel that this creates inconsistencies in the Standard language as well as potential Compliance Enforcement issues in reference to those particular Requirements (jumping from plans to a policy).

For SDT consideration, there is no access control requirement today for Low Impact Interactive Remote Access which expands the scope broadly to existing CIP standards. This is a similar concern for patching updates (patch management) for Low Impact BCS.

NRG is concerned that in R5.2 the term “controlling” implies operational and technical controls which is inconsistent with a policy level requirement.

Likes 0	
Dislikes 0	

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

- Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.
- To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

9. Does R5 allow the Entity to “accept the risk?”

10. R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

11. Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	

Same as RoLynda Shumpert's comments from SCE&G:

With the applicability of low impact BES Cyber Systems, this appears to negate a comment in CIP-002, R1.3 where it states, "… (a discrete list of low impact BES Cyber Systems is not required)".

What is the timing of R5.1 in terms of new software and existing software? The rationale explains that this starts in the operate/maintain phase of the life cycle but does the timing/life cycle language need to be added to the Standard rather than explained in the rationale section, which may not appear in the final language? Does this apply only to devices in production? For example, what if software is pre-loaded by an OEM. Is there an expectation that the Regional Entities work with their OEM to verify integrity and authenticity prior to this pre-loading? We seek more clarity in the language of R5 and recommend adding "…for Cyber Assets in production."

Regarding the security controls for vendor initiated and system-to-system remote access, R5 is about one or more documented policies and R4 is about the processes for authorization, logging and monitoring, and de-provisioning of remote access. With the requirement of one or more documented cyber security policy, how would Responsible Entities enforce the policy(ies) without also requiring documented plan(s) and process(es), which R5 does not address?

There is no need to have R5 because coverage of low impact BCS is already included in R1. There are two options for R5: integrate it into either (1) existing applicable NERC CIP Standards or (2) R2, R3, and R4 of CIP-013-1.

For option #2:

R2 is about the periodic review and approval of the supply chain cyber security plan(s) developed in R1. R3 obligates Entities to define process(es) to verify the baseline components and any upgrades prior to BCS installation. Requirement R5.1 appears to be identical to R3 because the term "software" in R5.1 is broad in scope and includes the OS and commercially available or open source software.

If Entities are concerned with R4.2 for low impact BCS, the integration of R5 and R4 can either include (1) "per Cyber Asset capability" or "if technically feasible" language for low impact devices or (2) specific language of a risk-based approach, vendor or system, in determining where remote access controls will be applied.

We recommend option #1, the removal of R5 from CIP-013-1 and integration of the requirement into existing applicable NERC CIP Standards.

Likes 0	
Dislikes 0	

Brad Lisembee - Southern Indiana Gas and Electric Co. - 6

Answer	No
Document Name	

Comment

We propose the SDT modify standard language based on Vectren's proposed language below:

R 5.

Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:

5.1 Review the vendor process for Integrity and verifying authenticity of software and firmware and any patches, updates, and upgrades to software and firmware, where a verification method is available from the vendor; and

5.2 Authenticating vendor-initiated remote access, including machine-to-machine remote access with vendor(s).

In the event the SDT does not accept the above changes, Vectren asks the following comments be considered:

R5

Integrity and authenticity concern as described in 1.2.5 above. Concerns that not all vendor products will provide a method to check authenticity.

Likes 0	
Dislikes 0	

Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	

Comment

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

2) If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

3) Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

4) R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches,

updates, and upgrades to software and firmware that are intended for use; and" As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

5) Concerned that in R5.2 the term "controlling" is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing "controlling"

6) Request that R5 be re-worded to mitigate risk like CIP-003 --- "organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems."

7) CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

Likes 0	
Dislikes 0	

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	No
Document Name	

Comment

R5 modifies requirements for the Cyber Security Policy, in conflict with CIP-003 R1. It also modifies the approval level required for a Cyber Security Policy (Senior Manager ONLY), allowing a delegate to approve part but not all of a Cyber Security Policy. The entire requirement belongs in CIP-003 and should be reworded to not undermine the governance structure set out in CIP-003 and the authority of the CIP Senior Manager.

CenterPoint Energy recommends that the SDT consider moving the portion of this requirement that is not duplicative to CIP-003 with the rest of the requirements for assets that contain Low Impact BES Cyber Systems.

Likes 0	
Dislikes 0	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUC is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. OUC requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, OUC requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	

Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	

CIP-003-6 R1.2 prescribes policy level controls. CIP-013-1 R5 effectively expands the requirements for policy beyond what is mandated in the current approved and enforceable version of the CIP-003-6 Reliability Standard. Any expansion in scope to CIP-related policy requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development, Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.

CIP-003-6 R2 requires registered Entities to develop and implement plans for the control of electronic access (which includes remote vendor-initiated user or system-to-system access) thereby rendering CIP-013-1 R5.2 superfluous and unnecessary, as well as placing it at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

CIP-003-6 R2 Attachment 1 Section 2 necessitates the implementation of electronic controls for low impact BES Cyber Systems in accordance with the plans developed pursuant to CIP-003-6 R2, thereby further rendering CIP-013-1 R5.2 superfluous and unnecessary, as well as placing it at odds with efforts associated to the FERC filing of proposed retired standards for Project 2013-02 Paragraph 81, and the intent to eliminate duplicative or unnecessary requirements that do not provide security or reliability value.

CIP-002-5 Requirement 1 R1.3 explicitly excludes the requirement for an inventory of low impact BES Cyber Assets through the its parenthetic clause stating, "**a discrete list of low impact BES Cyber Systems is not required**" and CIP-013-1 R5.1 effectively expands this current approved and enforceable requirement through its detailed Cyber Asset-level expectation related to software and firmware and any patches, updates, and upgrades to software and firmware. Any expansion in scope to policy requirements or controls for low impact BES Cyber Systems as defined in the currently approved and enforceable Standard should be subject to the Standards Authorization Request, Development,

Commenting, and Balloting Processes so as not to be effectively revising an existing approved and enforceable Reliability Standard through the creation of a separate one.	
Likes 0	
Dislikes 0	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	

Dislikes 0	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	
1. Supply chain risks may include insertion of counterfeits, unauthorized production, tampering and theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the industrial supply chain. Threats and vulnerabilities created by malicious actors (individuals, organizations, or nation states) are often especially sophisticated and difficult to detect, and thus provide a significant risk to organizations. It is difficult to understand how a low impact entity will be able to detect these risks and protect themselves against code that they have no control over. ACES recommends an approach that allows the vendors a process to communicate with low impact entities on how their product is secure. The vendor should be the focal point not low impact entities who do not have the resources to interact with multiple vendors constantly.	
Likes 0	
Dislikes 0	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016.

Reclamation recommends that Requirement R5 be deleted. There would be no need for Requirement R5 if all aspects of the supply chain risk management plan(s) are to be addressed in Requirement R1 and its sub-requirements.

Likes 0	
Dislikes 0	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Rationale for Requirement R5:

The rationale language for R5 states, “An entity could apply process(es) used for Requirements R3 and R4 to satisfy its obligations in Requirement R5.” IPC does not see this language reflected in the R5 requirement language. If documented processes are an acceptable means of achieving compliance with R5, IPC suggests rewriting the R5 requirement language to include the terms “processes” or “policies.” Additionally, there is continued creep in the standard language (here and elsewhere) to add requirements for Low Impact BCS, when Responsible Entities are still explicitly not required to have an inventory of Low Impact BCS. If it is the intent of the SDT and regulators to continue adding requirements to Low Impact BCS, IPC recommends a re-write of CIP-002-5.1 to ensure that all Low Impact BCS are appropriately identified rather than using standards to disagree with current enforceable standard language.

R5

The language of R5, R5.1, and R5.2 state, "Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

"**5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and

"**5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)."

IPC does not feel CIP-013-1 is an appropriate standard to address R5, R5.1, and R5.2. IPC believe R5, R5.1 and R5.2 belong in CIP-003-7(i), as R5, R5.1, and R5.2 are related to cyber security policies and low impact BES Cyber System requirements. IPC feels the intent of CIP-013-1 is to address supply chain controls, whereas CIP-003-7(i) addresses cyber security policies (High, Medium and Low) and all low impact BES Cyber System requirements.

IPC feels the requirement to have a policy reviewed by the CIP Senior Manager or delegate is purely administrative and does not provide value and recommends that it should be removed.

Likes 0	
Dislikes 0	

Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper

Answer	No
Document Name	

Comment

Santee Cooper is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Santee Cooper requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate

compliance without compiling a list. In addition, Santee Cooper suggests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
This requirement should be placed within CIP-003 alongside other requirements applicable to Low Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA recommends moving R5 to CIP-003 as it applies to Lows only. This will maintain the single standard requirement for entities that only have Low assets. The application of the requirement is not aligned with the current Low Impact BES Cyber System standard CIP-003 that does	

not require an inventory of equipment and software or identifying system cyber assets. Language and scope should be modified to provide clear scope and compliance requirements.	
Likes 0	
Dislikes 0	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	
1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003. 2) R5.1 is not consistent with R1.2.5, should R5.1 include the term “that are intended for use” to read “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” 3) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls R5 needs to be a process not a policy. If this is a policy, then suggest removing “controlling” 4) There should be exclusion comparable to a CIP Exceptional Circumstance added to this requirement for situations where the vendor does not cooperate or is otherwise unavailable. 5) R5 should be a plan document and not a policy document.	
Likes 0	
Dislikes 0	

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Colorado Springs Utilities (CSU) is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. CSU requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, CSU requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
Seattle City Light is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. Seattle City Light requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, Seattle City Light requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Jay Barnett - Exxon Mobil - 7	
Answer	No
Document Name	
Comment	
It is unclear how the risk and requirements in R5 for Low Impact BES Cyber Systems are differentiated from the other requirements and how the requirements will be measured considering a list of Low Impact systems are not required. There seems to be some reduncancy between R1 and R5 for Low Impact. Suggest removing Low Impact requirements from CIP-013 and incorporating into CIP-003 for consitency.	
Likes 0	
Dislikes 0	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Why not address this as part of the Cyber Security policy for Low Impact in R1.2 of CIP-003? Also what about the Cyber Security Policy for Highs and Mediums? Should that also address Supply Chain?	
Likes 0	
Dislikes 0	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	
The NYPA Comments	
Likes 0	
Dislikes 0	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
SMUD is concerned with R5 as there is not currently a requirement to conduct an inventory of equipment and software or identify systems. SMUD requests that the SDT clarify measures that would serve as evidence as it is not fully understood how to demonstrate compliance without compiling a list. In addition, SMUD requests that all requirements related to low impact assets be included in CIP-003.	
Likes 0	
Dislikes 0	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.	

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3. We recommend that the SDT consider deleting Requirement R5.	
Likes 1	Webb Douglas On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3
Dislikes 0	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC. In addition, it should be noted that CIP-003 R2 requires a plan, while CIP-013 R5 requires a policy. Where LPPC's comments request "that all requirements related to low impact assets be included in CIP-003," this can be accomplished by having the policy language as a portion of CIP-003 R1 part 1.2.	
Likes 0	
Dislikes 0	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No

Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
This requirement should be placed within CIP-003 alongside other requirements applicable to Low Impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3.

We recommend that the SDT consider deleting Requirement R5.

Likes 0	
Dislikes 0	

William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	

Comment

R1 and R2 are sufficient for addressing vendor risk for LIBCS. Requirements R1 and R2 require Responsible Entities to assess and evaluate ways to mitigate vendor risk. These requirements include LIBCS in addition to MIBCS and HIBCS. We do not believe that extending the operational controls (i.e., authenticity/integrity and remote access) to LIBCS is commensurate with the risk. If the SDT thinks the risk to LIBCS is significant, we encourage them to articulate this risk and how it outweighs the compliance burden created in addressing tens of thousands of LIBCS systems. Also, given the complications we raised above regarding compliance with these operational controls for HIBCS and MIBCS, we recommend that the SDT consider deleting R5.

We also note that vendor-based and equipment-based approaches that may be adopted for Requirements R3 and R4 are also likely to further address LIBCS. And part 5.2 is also duplicative with CIP-003-7, Attachment 1, Sections 2 and 3. We recommend that the SDT consider deleting Requirement R5.	
Likes 0	
Dislikes 0	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
We strongly disagree with requirement R5. The issues with this requirement are too many to list. In particular the SDT should avoid developing mandatory requirements that will reduce the security and reliability of the Bulk Electric System as it has proposed in this instance. The directive in FERC Order 829 is limited to "the context of addressing supply chain management risks." According to the definition of supply chain provided in NIST-800-53 (and referenced by FERC in paragraph 32, footnote 61), supply chain ends at the "delivery of products and services to the acquirer." In the system lifecycle, the supply chain management process occurs prior to the identification of a Cyber Asset as a BES Cyber System pursuant to the implementation of CIP-002-5.1a. This designation must only occur "upon commissioning" for planned system installations (and even later for unplanned changes). Therefore, this BES Cyber System identification, nor its categorization as low impact, does not exist during the supply chain context. Further, no list of low impact BES Cyber Systems is required. In order to demonstrate compliance with R5, entities would need a list of low impact BES Cyber Systems along with a full system baseline. The net effect of this requirement will be a SIGNIFICANT reduction in security by providing a regulatory disincentive to patch known security vulnerabilities in low impact BES Cyber Systems.	
Likes 0	

Dislikes 0	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The expectations for R5.1 are out of Entity scope for the reasons stated challenging R3. However, Low Impact BCS software and firmware should be expected to be checked for functionality by the Entity.	
Likes 0	
Dislikes 0	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	

Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
As this Standard is supposed to be focused on the vendor and as supply chain management risks apply equally to all categorizations of BES Cyber Systems, these requirements are superfluous. Requirement R1 already applies to all BES Cyber Systems and includes these requirement elements. There is no reason to call out requirements specific to Low Impact BES Cyber Systems. If the elements of the plans and processes are vendor-focused as they should be, there is no need to itemize the Low Impact BES Cyber Systems, which is the apparent real reason for Requirement R5 being defined separately.	
Likes 0	
Dislikes 0	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) The industry and previous drafting teams approved the concept that all standards that impact low impact asset be contained in CIP-003. Recommend moving CIP-013 R5 to CIP-003 R1.2 and if applicable, R1.1.

2) If the intent of R5 is the same as R3/R4 for the High/Medium then R5 should require “one or more documented processes” and not a policy.

3) Request clarification. To be the consistent with the policies approval in CIP-003 R1, then only the CIP Senior Manager can approve (not a delegate). Is this the SDT’s intent?

4) R5.1 is not consistent with R1.2.5. Recommend changing R5.1 from “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and“ to “Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware that are intended for use; and” As written R5.1 expands the scope or R1.2.5 with little increase to security or reliability

5) Concerned that in R5.2 the term “controlling” is not defined and is not consistent with the High/Medium language in R4. As an implementation of operational controls, R5 needs to be a process not a policy. If this is a process, then recommend removing “controlling”

6) Request that R5 be re-worded to mitigate risk like CIP-003 --- “organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems.”

7) CIP-013 R5 duplicates CIP-003 R2, which could result in the potential for multiple violations. CIP-013 R1.2.6 covers a policy while CIP-013 R5 is more of a plan

We are concerned that this requirement requires vendor cooperation or else it may not be possible to verify the integrity or authenticity of software and firmware provided by the vendor. Vendors do not fall under the jurisdiction of NERC.

· Request “per system capability” wording for R5. Not all vendors provide a “golden hash” or other mechanism to validate.

· To be consistent with not requiring R1.2.5, we suggest adding the language “subject to procurement contract.”

Does R5 allow the Entity to “accept the risk?”

R5.2 should be revised to say, “Ability to disable or otherwise respond to detected unauthorized activity during remote access sessions.”

Language of R5 should say “…shall document and implement one or more cyber security policies…” to clarify that implementation is expected for compliance. Draft R5 language does not include the term “implement”.

Likes 0	
Dislikes 0	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6

Answer	No
Document Name	

Comment

This requirement implies larger burdens on Low Impact BES Cyber Systems than the upcoming CIP-003-7 changes in regards to patch management and tracking. In neither of the previous versions of CIP-003, was it deemed necessary for patch management controls to be applied to Low Impact BCS. The nonvariable nature of the phrase "…and **any** patches, updates, and upgrades…" states that the Policies implemented to address this requirement will require a validation on every asset with a Low Impact rating. We recommend removing this Requirement and addressing the FERC Directive solely through R1.

Likes 0	
Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
The expectations for R5.1 are out of scope for and Entity for the reasons stated disputing R4. Low Impact BCS software and firmware should be expected to be checked for functionality by the Entity.	
Likes 0	
Dislikes 0	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
SunPower believes all Low Impact BES Cyber System Controls should go into CIP-003 R1.2, not create a new Requirement under CIP-013.	
Likes 0	
Dislikes 0	

Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Kansas City Power and Light Company incorporates by reference Edison Electric Institute's comments to Question 5.	
Likes 0	
Dislikes 0	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
As currently written, R1 and R5 are applicable to low impact BES Cyber Systems. R5 requires "one or more documented cyber security policies" while R1 requires "one or more documented supply chain risk management plan(s)". CIP-003 requires first a policy and then a plan. Policies are typically higher level documents than plans so consistency is an issue here. R5 is duplicative of the review and approval by CIP Senior Manager required in R2. For consistency with other CIP Standards, CIP-003 R1.1 should be expanded to include supply chain risk management as part of the collective cyber security policies to be reviewed and approved by the CIP Sr. Manager at least every 15 months and removed from CIP-013-1.	

R5.1 indicates a protection that needs to be applied at the Cyber Asset level, yet R5 is applicable to BES Cyber Systems. This language elevates low impact BES Cyber Systems to the level of medium and high impact BES Cyber Systems. Under existing CIP Standards, Security Patch Management requirements reside in CIP-007 and none are applicable to low impact BES Cyber Systems. Additionally, software and patching typically occurs at the Cyber Asset level and low impact entities are only required to identify assets containing low impact BES Cyber Systems. Implementing R5 applies controls from existing CIP Standards which are not applicable to low impact BES Cyber Systems. It is incongruous to require verification of patches on a low impact BES Cyber System for which there is no requirement to patch. For consistency purposes, this requirement should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to have a single place to for security plan requirements.	
Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
- Regarding R5.1, the Standard Drafting Team should clarify what is intended by “[I]ntegrity and authenticity.” This is an ambiguous term which can have different meanings. - Regarding R5.1, vendor information is proprietary (contractually). Registered Entities should not be held accountable for compliance obligations in which they have no control of. - Requirements pertaining to BES Low Impact Cyber Systems should be placed within CIP-003 Attachment 1 as originally intended.	
Likes 0	

Dislikes 0	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC

Answer	No
Document Name	

Comment

As drafted, R5 greatly increases the requirements for low impact BES Cyber Systems and completely ignores the H/M/L impact model. We feel there should be no such requirements for assets deemed to have a low impact on the BES, and that R5 should be struck entirely. If the SDT disagrees, then please clarify how implementation of these requirements would differ for low impact versus a medium or high impact system?

In addition, Tri-State is struggling to see how implementation of this requirement could be accomplished without a maintained inventory of low impact BES Cyber Systems, vendors, and software. This would be an incredibly substantial effort, that we believe the previous V5 drafting team understood well, which is why entities are not required to have a list of low impact BES Cyber Systems. Please clarify how an entity would carry out such policies while keeping with a low risk model.

Likes 0	
Dislikes 0	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray

Answer	No
Document Name	

Comment

Concur with EEI's Position	
Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
SVP agrees with other entities that requirements imposed on low impact assets be contained in CIP-003.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

NRECA recommends that CIP-013-1 R5 be placed within CIP-003 in order to keep consistency with the approach used in the remaining CIP standards. Low impact requirements were placed in CIP-003 in order to keep all requirements within a single standard and requirement. By adding these requirements into a new standard, there is confusion resulting in unnecessary compliance confusion.	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No
Document Name	
Comment	
This requirement should be eliminated in its entirety. We have adequate cyber controls in place for low impact Cyber Systems. The classification recognizes that these systems inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on each of the proposed requirements.	
Likes 0	
Dislikes 0	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
As with other comments, this requirement is duplicative and should be placed within the security plan under CIP-003 Attachment 1 for low impact BES Cyber Systems. Current standards have been drafted to allow entities with low impact BES Cyber Systems to refer to a single standard to for security plan requirements.	
Likes 0	
Dislikes 0	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	

Southern Company disagrees with the direction the proposed R5 requirement is taking, specifically with regard to the implied requirement to have a system baseline inventory of software and/or firmware on each Low Impact BES Cyber System when such an inventory is explicitly not required by existing CIP Standards. Not only does this create a collision of Standard requirements, but the burden on Responsible Entities would be immense and unmanageable – significantly increasing risk to reliability. Despite interpretation of language in this FERC Order, previous commission Orders have supported not requiring inventories at the Low Impact level. Southern recommends the comments previously provided under R1 to properly scope this Standard to "industrial control system" vendor products and services, within the Supply Chain horizon, where risk to assets containing Low Impact BES Cyber Systems is more appropriately addressed.

If the SDT chooses to keep R5 in the Standard in this manner, Southern provides the below edits to more appropriately scope this requirement towards the ICS vendor products at "assets containing lows." Again, consideration must be given to modifying this requirement language in a manner that does not introduce an implied responsibility to maintain an inventory of Low Impact BES Cyber Systems, their member Cyber Assets, and/or the individual component software and firmware baselines of those System components.

For example, if an entity has a thousand or more substations, it does not require a device level inventory of all devices in all substations to know the few vendors of relays that would be in those substations. Therefore, the entity would need to document how they deal with the firmware upgrades for those vendors. The same goes for generating plants; the entity does not need to know the thousands of individual devices in a plant to know the DCS or turbine control vendors per unit. Therefore, having plans and controls for dealing with the software, services, and remote access for those vendors is what is needed.

Additionally, Southern Company disagrees with the placement of this requirement, should it remain in this Standard, recognizing the SDTs time constraints with having to file a new or modified Standard addressing Supply Chain cyber security risks as per the FERC Order. Any requirement addressing controls for assets containing Low Impact BES Cyber Systems should be placed in CIP-003-6 R2, Attachment 1.

Modify R5 language as follows:

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics, based on risk, for its industrial control system vendor products and services at assets containing low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

5.1. Integrity and authenticity of software and firmware and any patches, updates,

and upgrades to software and firmware; and **5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).	
Likes 0	
Dislikes 0	
Louis Guidry - Louis Guidry On Behalf of: Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	

Dislikes 0	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
The proposed application of specific requirements to Low Impact BES Cyber Systems in CIP-013-1, R5 appears reasonable.	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
While in Agreement with the concept of adding a Requirement for low impact BES Cyber Systems, ACEC does have the following concerns: 1. Part 5.1 requires the Responsible Entity to have one or more cyber security policies for "Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware." This requirement is not consistent with CIP-002-5.1 which states in Requirement 1, Part 1.3 that "a discrete list of low impact BES Cyber Systems is not required." To be able to track security patches and firmware upgrades you will by necessity have to have a discrete list. It is recommended that Part 5.1 be replaced with the Information	

system planning security controls: this will ensure that security will be part of the planning for low impact Information Systems/Control Systems. 2. Part 5.2 requires the Responsible Entity to have one or more cyber security policies for "Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)." At present, CIP-003-6 Attachment 1, Section 3 requires only that you (3.1) "For LERC, if any, implement a LEAP to permit only necessary inbound and outbound bi-directional routable protocol access;" and "Implement authentication for all Dial-up Connectivity, if any, that provides access to low impact BES Cyber Systems, per Cyber Asset capability." This new Requirement extends these controls significantly beyond the present CIP-003-6 requirement and should be replaced with the Vendor risk management and procurement security controls: this will ensure that these issues are addressed early in the procurement process and throughout the lifecycle of low impact BES Cyber Systems and their associated Cyber Assets. 3. This Requirement should be moved to CIP-003-6, where ALL low impact BCS Cyber Systems security controls are addressed. This will allow Registered Entities with only low impact BES Cyber Systems to address only CIP-002-5.1 and CIP-003-6, reducing the potential for confusion. This approach has been taken by SDT 2016-02 in adding Transient Cyber Assets/Removable Media requirements to CIP 003-6 vice including in CIP-010-2 where it is addressed for high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
Should a reference to cyber security policies related to this Requirement for Low-impact BCS also be incorporated into CIP-003-7(i) R1.2?	
Likes 0	

Dislikes 0	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	Yes
Document Name	
Comment	

In the VSL for Requirement R5 there is no recognition of a Responsible Entity that had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, but the approval was more than 18 calendar months. A third entry should be added to the Severe VSL for Requirement that reads:

The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however, the approval was more than 18 calendar months from the previous review.

Likes 0	
Dislikes 0	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	

AZPS understands the time constraints associated with the development of this proposed standard, but respectfully asserts that all policy-related obligations should be consolidated into the appropriate requirements of CIP-003. AZPS, therefore, recommends that, upon

completion of this standards process, a SAR is entered to consolidate policy-related requirements such as Requirement R5 the existing CIP-003 Requirement R1.2	
Likes 0	
Dislikes 0	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
PSEG agrees with the intent of this requirement, but has the following questions/recommendations below: • Recommend moving CIP-013 R5 to CIP-003 R1.2, to remain consistent with previous decisions to maintain all low impact requirements in CIP-003. • Request clarification. Requirement R5 requires one or more documented policies. The Rationale for Requirement R5 states "An entity could apply process(es) used for Requirement R3 and R4 to satisfy its obligations in Requirement R5 or could develop a separate policy or processes to address low impact BES Cyber Systems." Is the intent of R5 similar to R3/R4 that the outcome is "one or more documented processes"? If so, should there be a separate policy requirement added to CIP-003 to have the CIP Senior Manager approve the policy?	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	

Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	
As the IESO does not have low impact Bes Cyber Assets we abstain from commenting on this requirement.	
Likes 0	
Dislikes 0	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Document Name	
Comment	
The IRC and SWG abstains from commenting on this requirement.	
Likes 0	

Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	

6. Do you agree with the Implementation Plan for proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan provide your recommendation and explanation.

Summary Consideration. The SDT thanks all commenters. The SDT has revised the Implementation Plan from 12 months to 18 months for CIP-013-1 in response to comments for longer implementation period. The SDT is proposing the same period for proposed CIP-005-6 and CIP-010-3. The SDT believes the revised Implementation Plan provides Responsible Entities with the necessary time to meet the requirements and will achieve the reliability objectives with due urgency.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

In light of the sweeping changes represented by CIP-013, potentially altering the way an entire industry assesses risk, deals with vendors and contractors, and performs security operations tasks, the 1 year after FERC approval effective dates are far too short for implementation. CenterPoint Energy would like to propose an effective date of at least 24 months following FERC approval. It will be a significant effort for entities to write a plan, negotiate with vendors, train and work with new groups to implement the requirements.	
Likes 0	
Dislikes 0	
Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	
1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems. 2) Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions. 3) Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”	
Likes 0	
Dislikes 0	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	
Comment	

Entergy seeks clarification on if the implementation date for CIP-013 merely requires that the entity have a CIP supply chain management plan in effect (with the ability to have a rolling implementation of specific protections and controls directed in that plan similar to the CIP-014 implementation), or if all protections and controls directed in the plan (including the potential technical deployment of new devices/systems) must be installed and live on day one of the implementation date. In other words, Entergy notes that the proposed standard recognizes and allows for a multi-phased, or rolling, implementation of the CIP supply chain management plan by not requiring contracts be renegotiated to adopt new terms and conditions; Entergy requests that CIP-013 explicitly allow entities to likewise have a phased or rolling implementation of identified controls and protections measures identified in their security plans after the implementation date.

In the alternative, Entergy cannot support the "12 month" implementation plan and recommends the date be no less than 18 months until more certainty on the extent of technical deployments required by the Standard can be provided. For example, until more clarity is given regarding whether implementation of existing CIP-005 and CIP-007 controls will adequately meet compliance with CIP-013 R4 and R5, or regarding the definition of "vendor remote access." This is because, depending on the date of passage, the 12 month implementation requirement may fall outside of an entity's capital planning and budgeting process, resulting in considerable constraints in acquiring funds for significant capital investment to achieve compliance with the standard.

Accordingly, Entergy requests that either a phased or rolling implementation be explicitly approved, or the implementation date be no less than 18 months.

Likes 0	
Dislikes 0	

Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	
Same as RoLynda Shumpert's comments from SCE&G: *With the inclusion of CIP-013 R1 through R5, SCE&G does not agree with the Implementation Plan. We agree with EEI's recommendation of extending the schedule from 12 months to 18 months.*	
Likes 0	
Dislikes 0	

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions.

Request clarification. The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”

The implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.

Likes 0	
Dislikes 0	

Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

In the implementation plan for this standard, NRG recommends a staggered implementation plan for R1, R2, & R5 being 15 calendar months. However, NRG recommends a 24-month implementation plan for R3 & R4would be needed for Registered Entities to manage this process on all impacted systems due to the need to re-negotiate processes with vendors (individualized solutions).

The implementation plan should have a timeline for compliance for initial enforcement and subsequent plan revisions – similar to CIP-002 with planned and unplanned changes.

In reference to R1 and contracts, we suggest that the term "future contracts" be addressed in the requirement language such as: "new or modified contracts" on or after the date of Enforcement. These should be vetted in an implementation plan. There will be a conversation of initial compliance versus implemented/ongoing compliance; therefore, NRG requests clear understanding of the implementation plan scope as it pertains to plan reviews, new contracts, modified contracts, and current contracts.

Likes 0	
Dislikes 0	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	

With the inclusion of CIP-013 R1 through R5, SCE&G does not agree with the Implementation Plan. We agree with EEI's recommendation of extending the schedule from 12 months to 18 months.

Likes 0	
Dislikes 0	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	

- Under General Considerations, additional language should be added to address existing contract extensions or addendums, effectively excluding them as well.

For the implementation plan which is 12 months, Dominion recommends an 18 month implementation period for the following reasons:

- Time is needed for entities to assess and impacted contracts relevant to applicable BES Cyber Assets.
- Budgets cycles often extend beyond a 12 month timeframe.
- New environments and assets may be in scope.
- This revision necessitate that entities conduct an impact assessment to determine what changes the revisions create and what is currently in place from the assessments performed for CIP version 6 implementation for low impact BES Cyber System.
- Revision iterations always require some time to assess and verify points of change.

Likes 0	
Dislikes 0	
Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	

Answer	No
Document Name	
Comment	
We do not support the implementation plan based on the proposed changes recommended in approach to addressing the directives. The implementation plan has to be revised to reflect a revised approach. Implementation of operational cyber security controls changes to standards CIP-002 through -011 should provide for at least two years, especially because of the time it may take some entities if they have to completely revise how their vendors are currently providing service to them.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	No
Document Name	
Comment	
Exelon generally agrees with the Implementation Plan for CIP-013-1 but offers the following recommendation for clarifying the plan for R2. The initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 must be completed within fifteen (15) calendar months **following** the effective date of CIP-013-1. There should be no obligation to review the plans ahead of time, and only the initial development and implementation should be required. This should be made clear in the Implementation Plan.	
Likes 0	

Dislikes 0	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
N&ST believes that 12 months from the Effective Date is too short for robust implementation. 18 months might be more appropriate.	
Likes 0	
Dislikes 0	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
Resilient Societies recommends a strategic reassessment of how NERC should, in good faith, respond to FERC Order No. 829. Many of the cost-effective remedial initiatives will be beyond the control of the North American electric utilities industry. Fundamental changes in the procurement of IT and OT systems will be required. Also, there are promising cross-industry initiatives to develop Open Source Codes that will better protect industrial control systems and other control systems upon which the electric utility industry depends. NERC should partici;pate in these ongoing initiatives. CIP-01301 imposes too large a burden on roughly 1400 electric utilities within the bulk electric system.	

Moreover, the Secretary of Energy has recently-granted (FAST Act) cyber security authority for the broader energy sector. Vulnerabilities of transmission and distribution utilities beyond FERC regulatory authority will foreseeably be channels through which foreign adversaries can attack the bulk electric system includng those portions that are subject to NERC-FERC standards. A broader framework is needed. The current draft Reliability Standard CIP-013-1 imposes substantial costs in time and money, and will not be a cost-effective initiative. We respectfully urge NERC to provide fresh guidance to the Standard Drafting team to link proposed reliability requirements to broader initiatives, includng the Defense Science Board Report of February 2017 and findings of the Trump Administratioon as it reviews cyber strategy and policy initiatives.This standard will be wasteful of resources, and is not ready for prime time.	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No

Document Name	
Comment	
R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems. Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions. R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard Implementation Plan refers to “contracts with vendors, suppliers or other entities”; however, Standard refers to only vendors in the text of the Requirements. “Suppliers or other entities” should be removed.	
Likes 0	
Dislikes 0	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Please refer to RSC- NPCC comments	
Likes 0	
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	
Based on FE’s comments on the Requirements (R1-R5), review of the Implementation Plan is not relevant at this time.	
Likes 0	
Dislikes 0	
John Hagen - Pacific Gas and Electric Company - 3	

Answer	No
Document Name	
Comment	
The implementation plan identifies that the effective date will be at least 12 months after the effective date of the applicable governmental authority's order approving the standard or 12 months after the date the standard is adopted by the NERC Board of Trustees where approval by an applicable governmental authority is not required. Extending the initial review and update, as necessary, of cyber security risk management plans specified in Requirement R2 by as much as 15 months after the effective date of the standard seems to extend the improved supply chain risk management unnecessarily. PGAE believes the initial review and approval of the cyber security risk management plans specified in R2 should be completed on or before the effective date, so that subsequent Requests for Proposal and/or vendor contracts and applicable Service Level Agreements after the effective date can incorporate the R1 controls.	
Likes 0	
Dislikes 0	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	
Since the effective date will be at least 12 months after NERC Board of Trustees approval under the current implementation plan, how does extending the initial review and update, as necessary, an additional 15 months provide for improved supply chain risk management? WECC believes the initial review and approval of the cyber security risk management plans specified in R2 should be completed on or before the effective date, so that subsequent Requests for Proposal [RFP] and/or vendor contracts and applicable SLAs after the effective date can incorporate the R1 controls.	

Likes 0	
Dislikes 0	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. SRP requests a 24-month implementation plan. SRP requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan. CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
Seminole does not believe that the standard is adequately defined to enable meaningful review of the implementation plan. Further, successful implementation of the plan is highly dependent on vendors and may require more than one year to implement.	
Likes 0	
Dislikes 0	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan. CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan. CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	

Dislikes 0	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems. Suggest breaking the implementation into three steps which follows CIP-014 – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities“ however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification.	
Likes 0	
Dislikes 0	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	

AE does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. AE requests a 24-month implementation plan. AE requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Tyson Archie - Platte River Power Authority - 5	
Answer	No

Document Name	
Comment	
PRPA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. PRPA requests a 24-month implementation plan. PRPA requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CHPD requests a 24-month implementation plan. CHPD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	

Likes 0	
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	

Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	
The implementation plan calls for R2 to be completed 15 months after the effective date of compliance of CIP-013; however, there is no requirement for signing the original R1 plan. Please clarify in R1 or R2 the required signature date for the supply chain cyber security plan.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy proposes an alternative Implementation Plan for the drafting team's consideration. We agree with an Implementation Plan of 12 months for R1 and R2, and propose an Implementation Plan of 24 months for R3 and R4. We feel that based on the type of work and the workload that will be necessary to comply with R3 and R4 due to these requiring technical controls and configuration changes, a longer implementation plan is required.	
Likes 0	
Dislikes 0	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
Suggest consider phasing the implementation of CIP-013 and CIP-003 Low BCS Physical, Electronic, TCA, and RM to reduce potential for resource constraints created by concurrent implementation of multiple programs.	
Likes 0	
Dislikes 0	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
The language in the Implementation - General Consideration refers to “contracts with vendors, suppliers or other entities, “however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.” Request clarification	
Likes 0	
Dislikes 0	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
Lack of a NERC definition of a PED makes it uncertain which products this (or any other) CIP standard applies-to. No new CIP standards should be developed until this issue is addressed. One year is not enough time, for the reasons stated above. A minimum of two years should be granted.	
Likes 0	
Dislikes 0	
faranak sarbaz - Los Angeles Department of Water and Power - 1	

Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item.	
Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	No

Document Name	
Comment	
12 calendar months may be inadequate if contracts are in the negotiation stage. 18 months may be more realistic; however, this is dependent on the language in the final set of requirements. We also recommend that the SDT consider how best to make it clear that this is a forward-looking standard as it relates to contracts, and the associated nuances. For instance, if you have a contract in place that allows for extensions or amendments, do you have to open up the entire contract when extending, making amendments, or minor revisions?	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No

Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
Due to the early stage of development of this standard, NRECA is not able to support a specific Implementation Plan.	
Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	

SVP agrees with other entities' comments to split the implementation plan into parts, e.g., identify risk, develop a plan and implement a timeline.	
Likes 0	
Dislikes 0	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

The Implementation Plan is unfeasible as currently drafted. The proposed Standard should utilize a phased in implementation. In addition, the Standard and Implementation Plan do not address that CIP-013 only addresses new contractual obligations. This lack of clarity will likely cause issues during the enforcement period of the Standard.	
Likes 0	
Dislikes 0	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
Oxy supports the comments of American Transmission Company, LLC	
Likes 0	
Dislikes 0	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	

Without being able to evaluate the Implementation Plan against the eventual final Standard, the company cannot offer its support.	
Likes 0	
Dislikes 0	

Bradley Collard - SunPower - 5	
Answer	No
Document Name	
Comment	
The technical controls required by R3/R4/R5 should be given additional time consideration. Perhaps 24 months to allow time to research and deploy technical controls of R3/R4/R5 while R1 – R2 are policy/contract-language driven only. Would a phased implementation approach be acceptable as a lot of the risks in R3, R4 and R5 have already been mitigated in CIP-007 and CIP-005 and therefore a maturity over time may make more sense?	
Likes 0	
Dislikes 0	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	

We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	No
Document Name	
Comment	
The Standards as currently written require significant modifications to organizational procurement processes for big and small entities alike. Due to the scope of assets being considered, entities must implement central procurement in such a way for every cyber asset to filter through the rigorous process. The number of contracts cutting across BES and non-BES Cyber Systems are too numerous and complex to address as a separate CIP compliance process. This has the potential to require more organizational change than any of the previous version of CIP Cyber Security Standards. In comparison, CIP version 5 implementation allowed for 24 calendar months and fully resourced entities struggled to get the organizational processes perfected in time to meet the deadlines. We propose a minimum of 24 calendar months be allowed for the currently drafted Standard. We feel this is appropriate given the minimal time FERC has permitted for this Standard to be submitted.	
Likes 0	
Dislikes 0	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No

Document Name	
Comment	
1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems. 2) Suggest breaking the implementation into three steps, which follows CIP-014 – Entity to a) identify risk, b) develop a plan, c) implement controls for contracts initiated after enforcement date and subsequent plan revisions. 3) Request clarification. The language in the Implementation - General Consideration refers to "contracts with vendors, suppliers or other entities "however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities." 4) Implementation Plan refers to "contracts with vendors, suppliers or other entities"; however, Standard refers to only vendors in the text of the Requirements. "Suppliers or other entities" should be removed.	
Likes 0	
Dislikes 0	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	

Dislikes 0	

Bob Reynolds - Southwest Power Pool Regional Entity - 10

Answer	No
Document Name	

Comment
The deferment of R2 by 15 months further supports the idea that the original documents do not have to be approved by the CIP Senior Manager, only subsequent revisions. The Implementation plan should at least require initial approval of the plans that are then subject to periodic review.

Likes 0	
Dislikes 0	

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment
GTC disagrees with the implementation plan. The security controls identified will take significant time to implement, particularly as specified for low impact BES Cyber Systems. The suggestion of a 12 month implementation window implies that fundamentally the SDT does not appreciate the volume and diversity of low impact BES Cyber Systems across North America. Additionally, a 12 month implementation window does not allow time for entities to complete an annual budget cycle. As such, we strongly recommend that the SDT considers an 18

month implementation window at minimum. If any controls are kept for low impact, then a minimum 24 month implementation window should be provided for those controls.

Alternatively, GTC recommends the SDT to work with NERC to immediately begin to take the necessary actions to request more time from FERC to satisfy Order 829. This can be accomplished in 2 phases.

For the first phase, GTC believes the 12 month implementation window can be achieved if the SDT would limit the structure of CIP-013-1 to the supply chain context which ends at the delivery of products/services to the acquirer in accordance with NIST SP 800-53 r4 as outlined in GTC comments number 1 and 3.

For the second phase, GTC encourages for NERC to lay out a plan to FERC to better address the operational/technical requirements of R3 and R4 with the applicable existing CIP standards so that the correct technical experts can develop in a manner that would not create the double jeopardy scenarios described under the comments for R4 and R5. NERC could then request a 24 month window to address the operational technical requirements in the correct applicable CIP standard. FERC provides NERC discretion per paragraph 44 the option of modifying existing Reliability Standards to satisfy the directive.

GTC recommends the SDT consider GTC's strategy in the comments above, and adapting the Implementation Plan accordingly.

Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Under initial performance, replace “of” with “following” so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…”

The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern.

We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification.

We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.

Likes 0	
Dislikes 0	

Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	

The IRC and SWG are unclear how an entity will comply with requirements in R3, R4, and R5 if contracts have not been renegotiated to address the requirements with vendors. Further, clear criteria needs to be identified to determine when an entity must comply with the requirements. The applicability of the Standard should be clarified to address cyber assets procured prior to the CIP-013 effective date. Concerns to be considered include, (1) upon execution of a new agreement with the vendor, (2) upon installation of any new equipment, or (3) upon installation of any new software? Requiring compliance on new equipment or software will be problematic if the contractual agreements do not align.

The IRC and SWG request a 24-month implementation timeframe for CIP-013 R3 and R4 as budget cycle(s) will be required to support contractual issues, implementation, with possible automation of compliance evidence.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
Under initial performance, replace “of” with “following” so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…” The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern. We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification. We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.	
Likes 0	
Dislikes 0	

Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
LCRA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. LCRA requests a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No
Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	

Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Under initial performance, we recommend replacing “of” with “following” so that it reads R2 must be completed within fifteen (15) calendar months following the effective date…” The general considerations section does not explicitly address contract term extensions or other amendments that would not involve renegotiating the contract. We recommend that the SDT add language to address this concern. We recommend 18 months rather than 12 so that contracts under negotiation can be included. Incorporation of an 18 month implementation plan is also in line with the changes recently approved by industry for the balance of the CIP Standards currently under modification. We also recommend that the SDT consider adding text to the requirements that make it clear that this is a forward-looking standard. Currently, this forward-looking information only appears in the implementation plan, which may become hidden or lost over time.	
Likes 0	

Dislikes 0	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	
Comment	
SMUD does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. SMUD requests a 24-month implementation plan. SMUD requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”	
Likes 0	
Dislikes 0	

Erick Barrios - New York Power Authority - 5

Answer	No
Document Name	
Comment	

The NYPA Comments	
Likes 0	
Dislikes 0	

Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	No
Document Name	
Comment	
Implementation plan must clearly state that all these requirements are forward looking and should not impact any existing contracts. We also believe that 12 months may not be enough to fully develop and implement a plan for large organizations to meet all four objectives. Perhaps a 24 month implementation period is appropriate. What is the difference between vendors, suppliers or other entities as stated in the implementation plan in the context of supply chain? None are defined terms.	
Likes 0	
Dislikes 0	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4;

Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No

Document Name	
Comment	
Seattle City Light does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Seattle City Light requests a 24-month implementation plan. Seattle City Light requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	
The IESO suggest that in order to be consistent with the FERC Order that the standards be forward looking, clear criteria needs to be identified to determine when an entity must comply with the requirements. The applicability of the Standard should be clarified to address cyber assets procured prior to the CIP-013 effective date. Concerns to be considered include, (1) upon execution of a new agreement with the vendor, (2) upon installation of any new equipment, or (3) upon installation of any new software? Requiring compliance on new equipment or software will be problematic if the contractual agreements do not align.	

The IESO request a 24-month implementation timeframe for CIP-013 R3 and R4 as budget cycle(s) will be required to support contractual issues, implementation, with possible automation of compliance evidence.	
Likes 0	
Dislikes 0	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	
Colorado Springs Utilities (CSU) does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. CSU requests a 24-month implementation plan. CSU requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to “contracts with vendors, suppliers or other entities” however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not “suppliers or other entities.”	
Likes 0	
Dislikes 0	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	No

Document Name	
Comment	
Recommendation for a 24-month implementation process. The implementation for the current CIP-013 standard is short. Many of the systems that are already in place under the current CIP standards were custom created or have features enabled to comply with the requirement(s) which they address. To comply with the standard requirements in CIP-013, in particular R4, registered entities may require modifications to the current processes and systems already in place or may require procurement of new components and/or services. The change process would require coordination with facility/equipment outages. A longer timeframe would be required for entities to effectively manage these changes without a negative impact to BES reliability. Also, to develop a supply chain risk management plan and implement that plan into our contracts would require more than 12 months to implement.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) R3/R4 implementation seems to make existing contracts applicable on the effective date of the Standard. Implementation of R3 would need to be done using the CIP-010 Cyber Security – Configuration Change Management process for managing changes to the baseline. A 24-month process would be needed for larger entities to manage this process on all impacted systems.

2) Suggest breaking the implementation into three steps which follows CIP-014 – Entity to 1) identify risk, 2) develop a plan, 3) develop an implementation timeline

3) The language in the Implementation - General Consideration refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities." Request clarification.

Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

BPA believes the lack of clear scope in the standard makes the evaluation of the implementation timeframe ambiguous. If the standard was adopted as written and required Low impact cyber asset inventories identification and evaluation, 24 months would be required to comply with the requirements.	
Likes 0	
Dislikes 0	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
LCRA does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. LCRA requests a 24-month implementation plan.	
Likes 0	
Dislikes 0	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	

Santee Cooper does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. Santee Cooper requests a 24-month implementation plan.

Santee Cooper requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."

Likes 0	
Dislikes 0	

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

In IPC's opinion, a 12 month effective date is not enough time to implement this standard given the amount of existing CIP standards currently in flux and new standards being developed. In addition, Regulatory guidance is often slow in coming, and entity budgetary cycles are usually at least 12 months. IPC suggests an 18–24 month effective date. An 18-month effective date is also consistent with the CIP-003-7 implementation plan.

Likes 0	
Dislikes 0	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends that the implementation schedule be based on risk and enforced using a systematic approach. Under the systematic approach, Reclamation requests that plans affecting high impact BES Cyber Systems would be developed within 12 months of FERC approval, plans affecting medium impact BES Cyber Systems would be developed within 18 months of FERC approval, and plans affecting low impact BES Cyber Systems would be developed within 24 months of FERC approval. Reclamation recommends that each plan should be implemented within 18 months of being developed.	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
It is premature to accept/agree with any implementation plan due to the infancy of this proposed standard and potential risks, impacts, and unintended consequences that may ensue if the CIP-013-1 Standard were to move forward without adequately addressing the concerns of redundancy, lack of clarity, expansion in scope, or contradictory nature of the collective set of proposed requirements as described in above comments. Until the language can be improved so as not to create double jeopardy or an impossibly of non-compliance due to factors outside the control of the Registered Entity, or until a shift in approach can be agreed upon so as to leverage existing enforceable regulations that already provide the intended security or reliability benefit, ATC cannot support the proposed implementation plan.	
Likes 0	
Dislikes 0	

Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUC does not agree that a 12-month implementation plan is sufficient. For example, if processes for verifying integrity and authenticity are to be implemented for each individual vendor, that could be an extraordinarily time consuming activity. OUC requests a 24-month implementation plan. OUC requests clarification on the language that is used to address vendors and suppliers. In the Implementation - General Consideration it refers to "contracts with vendors, suppliers or other entities" however, the Standard only refers to vendors. The Rationale for R1 defines vendors but not "suppliers or other entities."	
Likes 0	
Dislikes 0	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
We feel that the approval of the RSAW needs to be included in the documentation. This is another document that is pertinent to the Implementation Plan Process.	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
The proposed 12-month implementation period and specification of an initial performance date for the CIP-013-1, R2 review and update appear reasonable. Texas RE requests the SDT provide a justification for the 12-month implementation period as part of the Standard development process.	
Likes 0	
Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	

Answer	Yes
Document Name	
Comment	
In conjunction with the comments provided under R1 above, Southern Company supports the SDTs direction proposed in the Implementation Plan where it is applicable to the Supply Chain time horizon and industrial control system vendor products and services used in BES Cyber Systems, but requests the consideration of an 18 month (rather than 12 month) timeframe. For any requirements applicable to assets containing Low Impact BES Cyber Systems, given the volume and complexity of those assets, as well as the volume and diversity of agreements necessary between the Responsible Entity and it's suppliers of ICS products and services, Southern requests the consideration of a 24 month timeframe for implementation.	
Likes 0	
Dislikes 0	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

George Tatar - Black Hills Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Kenya Streeter - Edison International - Southern California Edison Company - 6	

Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	

Twelve months is not sufficient time to allow compliance with all aspects of this standard. The drafting team should consider a phased approach allowing the logical phased implementation of these requirements. While the Implementation Plan suggests that existing contracts need not be modified, the proposed standard language does not make this clear. ERCOT believes the standard to be a more appropriate location for this exemption, as it is ultimately substantive in nature. ERCOT there recommends that the drafting team include language in the standard explicitly limiting applicability of the requirements to new contracts.	
Likes 0	
Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	

7. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the requirements in proposed CIP-013-1? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs provide your recommendation and explanation.

Summary Consideration. The SDT thanks all commenters. The SDT is not proposing any changes to CIP-013-1 VRFs. The SDT has revised VSLs for clarity and to specify additional levels of compliance, where appropriate.

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	

Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The VLS for R1	

- The term “Either of the elements specified” in the Sever VLS is implying two elements when in fact I believe you are meaning “Any of the Elements in Either of the two requirement subparts.”
- The High VLS specifies “…did not include one of the elements specified in Parts 1.1 or 1.2”. Since one of these elements 1.2.7 is optional by inclusion of the “if applicable” language, this VLS should be rewritten to specifically exclude 1.2.7.

The VSL for R2

- Reviewing and modifying the plan reduce the risk, having a signature does not. Setting arbitrary times frames surrounding missing dates does not reduce risk. Recommend:

o VSL lower - no signature

o VSL Moderate - missing a new supply chain security risk during the review

o VSL High - not performing review within 15 months

o VSL Sever - not implementing needed control changes as identified from review

Likes 0	
Dislikes 0	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	

Likes 0	
Dislikes 0	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

VSL for Requirement R3

Requirement R3 has four sub-parts which describe the software and firmware which need to be verified. ReliabilityFirst recommends the SDT structure the VSLs similar to Requirement 1 to address each of the sub-parts. ReliabilityFirst offers the following modifications for consideration

Lower VSL – The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify one of the elements specified in Parts 3.1 through 3.4.

Moderate VSL - The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify two of the elements specified in Parts 3.1 through 3.4.

High VLS – The Responsible Entity implemented one or more documented process(es) for verifying the integrity and authenticity of the software and firmware but did not verify three of the elements specified in Parts 3.1 through 3.4.

Severe VSL - The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.

VSL for Requirement R5

To account for instances where the Responsible Entity had cyber security policies specified in the requirement but were not reviewed for 18 months or greater, ReliabilityFirst recommends the following “OR” statement be added to the Severe VSL Category: Additional Severe VLS - The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 18 calendar months from the previous review.	
Likes 0	
Dislikes 0	
ALAN ADAMSON - New York State Reliability Council - 10	
Answer	No
Document Name	
Comment	
See NPCC comments.	
Likes 0	
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Mark Riley - Associated Electric Cooperative, Inc. - 1	
Answer	No
Document Name	
Comment	
AECI does not agree with the requirements as written and accordingly cannot agree with the proposed VRFs and VSLs proposed for those requirements in CIP-013-1.	
Likes 0	
Dislikes 0	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Tyson Archie - Platte River Power Authority - 5

Answer	No
Document Name	

Comment

PRPA does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, PRPA requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. PRPA requests considering all of

the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Andrew Gallo - Austin Energy - 6	
Answer	No
Document Name	
Comment	

AE does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, AE requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. AE requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	No
Document Name	

Comment

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3 and R4: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but

not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

Do not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

Likes 0	
Dislikes 0	

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	
W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	

Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Seminole does not believe that the standard is adequately defined to enable meaningful review of the VRF and VSL.	
Likes 0	
Dislikes 0	

Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	

Likes 0	
Dislikes 0	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

CHPD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CHPD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CHPD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
SRP does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, SRP requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. SRP requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	

Comment
WECC believes missing one of the elements of Part 1.2 in the VSL for Requirement R1 should be considered lower risk than missing one of the elements in Part 1.1, as it seems to be a subset of Part 1.1., and should be assessed at moderate risk. WECC agrees that missing one of the elements of Part 1.1 is appropriately identified as a High VSL. In the VSL for Requirement R5 there is no language for a Responsible Entity that had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, but the approval was more than 18 calendar months from the previous review. WECC believes a third entry should be added to the Severe VSL for Requirement that reads:

The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however, the approval was more than 18 calendar months from the previous review. Additionally, in the high and severe VSL language of R5 it appears that the word "but" before the words "did not include" should be deleted.	
Likes 0	
Dislikes 0	
John Hagen - Pacific Gas and Electric Company - 3	
Answer	No
Document Name	
Comment	
PGAE believes missing one of the elements of Part 1.2 in the VSL for Requirement R1 should be considered lower risk than missing one of the elements in Part 1.1, as it seems to be a subset of Part 1.1., and should be assessed at moderate risk. We agree that missing one of the elements of Part 1.1 is appropriately identified as a High VSL.	
Likes 0	
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	

Based on FE's comments on the Requirements (R1-R5), review of the VRFs and VSLs is not relevant at this time.	
Likes 0	
Dislikes 0	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	

Dislikes 0	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
We have not reviewed with care, but consider the standard requirements need fundamental reworking before addressing VRFs and VSLs.	
Likes 0	
Dislikes 0	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
There is a concern that there is an inconsistency with the risk impact classification for the Requirements, and VSLs. We feel that these inconsistencies have the potential to lead to Compliance Enforcement issues in reference to the proper alignment of both sections. For example, the VSLs for Requirement R3 and Requirement R4 focus on high and medium, however, Requirement R5 mentions low impact. We feel that all three (3) classifications need to be considered in all of the Requirements language to have a successful Standard.	
Likes 0	
Dislikes 0	

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	
The VRFs and VSLs will need to be incorporated in CIP-002 through -011 where changes are made.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No
Document Name	
Comment	
• We recommend that requirements R1 and R2 should be low based on the fact the requirements are administrative in nature (i.e., deal with the procurement), and if violated, would not be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor and control the Bulk Electric System; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the Emergency, abnormal, or restorative conditions anticipated by the	

preparations, be expected to adversely affect the electrical state or capability of the Bulk Electric System, or the ability to effectively monitor, control, or restore the Bulk Electric System. • We recommend that requirement R5 should be Low because it is related to CIP-003-6 which is also Low.	
Likes 0	
Dislikes 0	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Due to our concerns expressed in this document, we did not find it useful to review the VRFs and VSLs at this time.	
Likes 0	
Dislikes 0	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

There is a concern that there is an inconsistency with what is stated in the Requirements, VRFs, and VSLs. These inconsistencies have the potential to lead to Compliance Enforcement issues in reference to those particular elements of the Standard and therefore, NRG recommends alignment between Requirements, VRFs, and VSLs. NRG suggests that this language be properly aligned with the requirements (recommendation for Low or Moderate VSLs relating to process controls) or else this could lead to future Compliance Enforcement issues for the industry.

Likes 0	
Dislikes 0	

David Rivera - New York Power Authority - 3

Answer	No
Document Name	

Comment

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the

implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted. For R4: See comment above for R3.	
Likes 0	
Dislikes 0	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	
Same as RoLynda Shumpert's comments from SCE&G: *Due to our concerns expressed in this document, we did not find it useful to review the VRFs and VSLs at this time.*	
Likes 0	
Dislikes 0	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	

The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	

Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	

1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

2) For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

3) For R4: See comment above for R3.

Likes 0	
Dislikes 0	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
The VRFs and VSLs seem harsh. CenterPoint Energy does not agree with the automatic High VSL for any element not fully addressed, in a Regional Entity's opinion, by a Responsible Entity's risk management plan, especially given the extremely vague bounds presented on what represents a valid risk management methodology, planning process, evaluation method, or mitigation effectiveness measure.	
Likes 0	
Dislikes 0	
Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	

Dislikes 0	
Ballard Mutters - Orlando Utilities Commission - 3	
Answer	No
Document Name	
Comment	
OUCX does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, OUC requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. OUC requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	

It is premature to accept/agree with the VRFs or VSLs due to the infancy of this proposed standard and potential risks, impacts, and unintended consequences that may ensue if the CIP-013-1 Standard were to move forward without adequately addressing the concerns of redundancy, lack of clarity, expansion in scope, or contradictory nature of the collective set of proposed requirements as described in above comments. Until the language can be improved so as not to create double jeopardy or an impossibly of non-compliance due to factors outside the control of the Registered Entity, or until a shift in approach can be agreed upon so as to leverage existing enforceable regulations that already provide the intended security or reliability benefit, ATC cannot support the proposed VSLs/VRFs.	
Likes 0	
Dislikes 0	
Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	

Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
The sub-requirements within each requirement should be used to distinguish the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).	
Likes 0	
Dislikes 0	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

IPC feels all VSLs should be set to low the first year of enforcement and then increase the VSL after year one of enforcement. This allows for process refinement without significant penalty.	
Likes 0	
Dislikes 0	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	
Comment	
Santee Cooper does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Santee Cooper suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Santee Cooper suggests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and constructs the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. LCRA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA suggests the VRFs and VSLs include consideration for instances where the vendor or supplier is not able or is unwilling to support the standard requirement.	
Likes 0	
Dislikes 0	

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

2) For R3 and R4: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

3) Do not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Suggests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

Likes 0	
Dislikes 0	

Glenn Pressler - CPS Energy - 1	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by APPA	
Likes 0	
Dislikes 0	

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	

Colorado Springs Utilities (CSU) does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, CSU requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. CSU requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

The IESO requests review to ensure violations align with impact ratings and existing standards program.

For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, policies and plans are implemented while processes are performed. If a policy or plan is required to be implemented and there is an instance where a process included as part of the policy or plan, is not adhered to, then this would result in a violation of the policy or plan but not in the requirement to implement the policy or plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted

For R4: See comment above for R3.

Likes 0	

Dislikes 0	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	
Seattle City Light does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, Seattle City Light requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late. For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. Seattle City Light requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	

FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	

The NYPA Comments	
Likes 0	
Dislikes 0	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD does not agree with the VSLs that classify a level of non-compliance as a High or Severe. In R2 and R5, SMUD requests that the SDT consider incrementally increasing the VSL for lateness based on a range (0-6 months = Lower, >6 = Moderate) instead of increasing the level of severity by each month late.

For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language “did not include either element” leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. SMUD requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

Likes 0	
Dislikes 0	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	
Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.	
Likes 0	
Dislikes 0	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC	
Answer	No

Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
For R1, it is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, as a minimum. LCRA requests considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No

Document Name	
Comment	
Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.	
Likes 0	
Dislikes 0	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	
The IRC and SWG requests review to ensure violations align with impact ratings and existing standards program. For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL. For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, policies and plans are implemented while processes are performed. If a policy or plan is required to be implemented and there is an instance where a process included as part of the policy or plan, is not adhered to, then this would result in a violation of the policy or plan but not in the requirement to implement the policy or plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a	

Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted For R4: See comment above for R3.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
Due to our concerns expressed above, we did not find it useful to review the VRFs and VSLs at this time.	
Likes 0	
Dislikes 0	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	

GTC recommends the SDT consider GTC's comments above, and adapting the VRFs and VSLs accordingly.	
Likes 0	
Dislikes 0	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The VRF mapping based on the ERO Final Blackout Report is questionable because CIP-013 only addresses the possible inclusion of non-authentic or compromised hardware, firmware, and software; and does not speak to the risk level of the inclusion. The same compromised hardware, software, or firmware will pose different risks to the BES based upon the inherent risk to the BES by the Entity. The VSL's are acceptable from a documentation administration standpoint, but do not correspondinly map to the impact resulting. While it is now appropriate to be generating ideas on VRF and VSL for CIP-013, a final determination should wait until the industry is closer to consensus on the actual requirements.	
Likes 0	
Dislikes 0	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	

Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	

Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Requirement R2 calls for the periodic review of existing plans and approval of updates. This is mostly a documentation management requirement and the VRF could be defined as Lower instead of Medium. Compromised software integrity is a key element of previous successful cyberattacks, including Havex. The VRF for Requirement R5 needs to be Medium even though the focus of the Requirement is on Low Impact BES Cyber Systems. The Severe VSL for Requirement R1 should refer to failing to include two or more elements of Parts 1.1 or R1.2. While that should be able to be presumed from the lesser applicability of the High VSL for R1, it is not sufficiently clear.	
Likes 0	
Dislikes 0	

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	

Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) For R1. It is unclear what is considered an element of Parts 1.1 and 1.2. The language for Severe uses the language "did not include either element" leading to the conclusion that R1.1 and R1.2 are the only two elements and that missing any one of the sub-requirements could be considered a failure to include the entire element and would result in a High VSL violation, at a minimum. Recommend considering all of the nine sub-requirements of R1.1 and R1.2 as separate elements and construct the VSL table to be consistent with CIP-003-6 R1.1 where missing a single element results in a Lower VSL.

2) For R3: It is unclear what the difference is between implementing a process and performing a process that has been implemented. In general, Policies and Plans are implemented while processes are performed. If a Policy or Plan is required to be implemented and there is an instance where a process included as part of the Policy or Plan, is not adhered to, then this would result in a violation of the Policy or Plan but not in the requirement to implement the Policy or Plan. The requirement to implement a process could result in a High VSL violation for each instance where the procedure was not followed. With this understanding, the single violation of following a process should not result in a Severe VSL. Suggest having the VSL level dependent on the number of failures to implement the process. This is consistent with the implementation of a process in CIP-002 resulting in a VSL level based on the number or percentage of instance the process was not conducted.

3) For R4: See comment above for R3.	
Likes 0	
Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	
Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
The VRF mapping based on the Final Blackout Report is questionable because CIP-013 only addresses the possible inclusion of non-authentic or compromised hardware, firmware, and software; and does not speak to the risk level of the inclusion. The same compromised hardware, software, or firmware will pose different risks to the BES based upon the inherent risk to the BES by the Entity. The VSL's are acceptable from	

a documentation administrative standpoint, but do not map to the risk presented. While appropriate to be generating ideas on VRF and VSL, final determination should wait until the industry is closer to consensus on the actual requirements.	
Likes 0	
Dislikes 0	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	

Without being able to evaluate the VRFs and VSLs against the eventual final Standard, the company cannot offer its support.	
Likes 0	
Dislikes 0	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	
Oxy does not agree with the proposed language of the requirements and therefore cannot agree with the VRF's and VSL's until requirements are revised and updated and corresponding updates are made to the VRF's and VSL's.	
Likes 0	
Dislikes 0	

Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	

Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	No
Document Name	
Comment	
-- See comments from APPA, with which SVP agrees.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
Due to the early stage of development of this standard, NRECA is not able to support a specific set of VRFs and VSLs.	
Likes 0	
Dislikes 0	

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes
Document Name	
Comment	
For R5, the mention of part 5.1 should be removed for High and Critical (see comments on R5 above).	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

No Comments	
Likes 0	
Dislikes 0	

Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	
Comment	
We agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs), provided that they should be updated to reflect changes to the proposed Standards Requirements consistent with the recommendations discussed in questions 1-6.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	

Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

In light of all previous comments made above, Southern Company requests that the SDT also consider the VSLs for R3, which should accommodate other levels of severity with regard to verifying integrity and authenticity of industrial control system vendor products, software, patches, and/or upgrades. As currently written, any violation of R3 is considered Severe. There are more granular levels of severity to be considered, for example – when a Responsible Entity has a plan(s), has implemented that plan(s), but a percentage of a volume of patches applicable to a particular business unit (out of many business units within a Responsible Entity) were not adequately validated.	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Scott Downey - Peak Reliability - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
N/A	
Likes 1	OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	

Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	

Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	
Document Name	
Comment	
Vectren does not vote in non-binding polls. (VRFs and VSLs).	

Likes 0	
Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	
These will be reviewed in-depth after changes are made to the requirements.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	

8. The SDT drafted the *Technical Guidance and Examples* document to provide entities with technical considerations and examples of controls that will aid in implementing proposed CIP-013-1. Provide any comments or suggestions to improve the document, including recommended changes, additions, or deletions, along with technical justification. Include page and line number if applicable.

Summary Consideration. The SDT thanks all commenters. The SDT developed draft Implementation Guidance from the Technical Guidance and Examples document. The SDT's intent is to provide considerations for implementing the requirements in CIP-013-1 and examples of approaches that Responsible Entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-1. The draft Implementation Guidance is intended to highlight some approaches that the SDT believes would be effective ways to be compliant with the standard, and will be submitted for ERO endorsement as described in NERC's Compliance Guidance Policy.

Dennis Sismaet - Northern California Power Agency - 6	
Answer	No
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

The Technical Guidance and Examples makes it more evident as to how much of CIP-013 is duplicative of exisiting CIP Standards. CenterPoint Energy strongly recommends that the CIP-013 draft be edited as noted and the Technical Guidance and Examples be revised accordingly.	
Likes 0	
Dislikes 0	
Quintin Lee - Eversource Energy - 1	
Answer	No
Document Name	
Comment	

1) The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.

2) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

3) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

4) Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

5) Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

6) Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

7) Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

8) Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

9) Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

10) Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

11) Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

12) Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

13) Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

1) Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

2) Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

3) Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems. 4) Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition. 5) Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”. 6) Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”. 7) Page 11, Line 15, replace supplier with Vendor. 8) Page 11, line 25, replace “should” with “may” 9) Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted. 10) Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine. 11) Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session? 12) Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity. 13) Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.	
Likes 0	
Dislikes 0	

Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	No
Document Name	
Comment	
Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document. **R1** R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?	

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle. 1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor? 1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates. 1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities. **R2** Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader. **R3** How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit? Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors. Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above. **R4** Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	No
Document Name	
Comment	

Same as RoLynda Shumpert's comments from SCE&G:

Although the Guidelines and Technical Basis document has been helpful, it will need further changes to reflect the changes in the requirements driven by concerns of Regional Entities.

Likes 0	
Dislikes 0	

David Rivera - New York Power Authority - 3	
Answer	No
Document Name	
Comment	

The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity. Page 15, line 23 Provide guidance on the meaning of "timely manner." Would responding to an issue discovered in a 30-day log review be considered timely? How does "timely manner" align with "during the remote access session" language of R4.3. Page 16 line 25, replace "should" with "may".	
Likes 0	
Dislikes 0	
RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC	
Answer	No
Document Name	
Comment	
Although the Guidelines and Technical Basis document has been helpful, it will need further changes to reflect the changes in the requirements driven by concerns of Regional Entities.	
Likes 0	
Dislikes 0	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6	
Answer	No

Document Name	
Comment	

- Recommend removing the responsible entities section in this document as the entities are already outlined in the Standard itself.
- Page 1 Line 42: additional language should be added to address existing contract extensions or addendums, effectively excluding them as well.
- Recommend revising this document based on the revisions made to CIP-013.

Likes 0	
Dislikes 0	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1	
Answer	No
Document Name	
Comment	

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle. 1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor? 1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates. 1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities. **R2** Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader. **R3** How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit? Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors. Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above. **R4** Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham	
Answer	No
Document Name	
Comment	
CIP-002 through -011 Guidelines and Technical Basis should be updated to reflect revisions to those standards and to ensure there is not conflicting guidance. Outside of the Guidelines and Technical Basis in the standards, other implementation guidance could be proposed for the ERO deference process.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey
Dislikes 0	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	No
Document Name	
Comment	
Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.	

R1

R1.2.2 – Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – Same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.	
Likes 0	
Dislikes 0	
Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	No
Document Name	
Comment	

Technical Guidance and Examples

Vectren understands the SDT is working on separating the Technical Guidance and Examples document into a Guidance and Technical Basis document and an Implementation Guide. Below are comments regarding the current document.

R1

R1.2.2 -- • Request vendor cooperation to obtain Responsible Entity notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems ("Security Event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. How does a vendor security event affect the availability or reliability of the BES Cyber Systems?

1.2.3 – Technical Guidance & Examples states that for the duration of the relationship with the vendor cooperation in access to documentation regarding identified security breaches. Standard states R1 and R2 are for the procurement (and deployment) of products, not the operate/maintain portion of the life cycle.

1.2.4 – same concern of how does a security event with an adverse impact to the availability or reliability of BES Cyber Systems require vendor cooperation on notification processes, assistance and support requirements from the vendor?

1.2.5 – Concerns requiring vendors to provide documentation on how to apply, test updates and patches. Concern with critical vulnerabilities being a shorter update period than allowed for other types of updates.

1.2.6 – Concern with requiring vendor to keep logs, etc. of connection access activities.

R2

Page 9, second line from bottom – R2 is overly broad and the industry best practices and guidance statement makes it broader.

R3

How would utility verify software to be installed was not modified without the awareness of the software supplier and is not counterfeit?

Concerns with items under Potential Software Integrity Controls on page 12 – validating the digital signature may not ensure the software's integrity – it is possible both the file and the signature could be compromised. Fingerprints or cipher hashes may not be available from all vendors.

Concerns with items under Potential Software Authenticity Controls on page 12 – same concern over digital signature, as above.

R4

Concern with ambiguity of requiring the Responsible Entity to monitor authorized/unauthorized (inappropriate) access.

Likes 0	
Dislikes 0	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

We feel that there is inconsistency with the language of the Requirements and The Technical Guidance language specifically in reference to Requirement R3 and Requirement R4. The guidance section for both Requirements mentions reviewing security policies. However, the Requirements mention Risk Management Plans. We feel that this language needs to be properly aligned or this will lead to future Compliance Enforcement issues for the industry.

Likes 0	
Dislikes 0	

OSI Open Systems International - OSI Open Systems International - NA - Not Applicable - NA - Not Applicable

Answer	No
Document Name	

Comment

As a vendor of SCADA/EMS/TMS systems for many NERC Responsible Entities, OSI (Open Systems International Inc.) is providing the following comments to the NERC CIP-013 SDT for consideration. All suggested text additions are identified in ***bold-italics*** font.

R1.1.1 Identify and assess risk(s) during the procurement and deployment of vendor products and services;

OSI recommends that the SDT consider an additional comment for paragraph 5 as follows:

Personnel background and screening practices by vendors. ***Note that state & local laws may prevent vendors from sharing certain private information about their employees as related to their background screening (eg. social security numbers).***

OSI recommends that the SDT consider an additional comment for paragraph 9 as follows:

System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout their processes. ***Vendor policies showing adherence to appropriate industry standards for secure development***

processes is an acceptable method for Responsible Entities to demonstrate due diligence. An example of acceptable industry standards for secure development are the various System & Services Acquisition (SA) controls related to SDLC within NIST 800-161.

Note that NIST 800-161 is the standard used by U.S. Government entities to ensure Supply Chain Security for all departments and sites.

OSI recommends that the SDT consider an additional comment for paragraph 10 as follows:

Review of certifications and their alignment with recognized industry and regulatory controls. ***It is important that Responsible Entities consider which industry certifications are applicable for each vendor's line of business and not use a "one size fits all" approach. For example, NIST 800-161, ISO-27001 are relevant standards pertaining to computer system security. On the other hand, inclusion of requirements for non-relevant or specialized certifications could disqualify certain vendors (eg. certifications used by the financial industry).***

R1.2 Potential Procurement Controls

It is OSI's opinion that the current CIP-013 non-prescriptive approach to the development of procurement controls will lead to an unsustainable permutation of controls and associated contracts for vendors supporting the industry. The extreme diversity of procurement controls/contracts may push certain vendors away from the bidding process, ultimately reducing competition and increasing costs for the industry as a whole. OSI strongly urges that NERC and the CIP-013 SDT consider the addition of acceptable examples of compliance for different classifications of industry vendors eg. SCADA software vendors, RTU vendors, transformer vendors, etc. NERC and Regional Entity endorsement of such examples will provide both vendors and entities with a sensible baseline for procurement controls. OSI is providing an example of guidance for SCADA/EMS vendors as follows:

The following represents example procurement controls that can be considered for EMS/TMS/SCADA system vendors. This set of controls is not the only method of achieving compliance, but it is considered by NERC to be one acceptable method.

The following "National Institute of Standards and Technology" (NIST) standards can be used to satisfy R1.2. Controls that are applicable to the EMS/TMS/SCADA vendor should be extracted from the various sections to utilize within a procurement contract for compliance with R1.2.

- ***NIST 800-161: "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"***

- ***AC – Access Controls***
- ***AT – Security Awareness and Training***
- ***AU – Audit and Accountability***
- ***CA - Security Assessment and Authorization***
- ***CM – Configuration Management***
- ***CP – Contingency Planning***
- ***IA – Identification and Authentication***
- ***IR – Incident***
- ***MP – Media Protection***
- ***PE – Physical and Environmental Protection***
- ***PL – Security Planning***
- ***PM – Security Program Management***
- ***PS – Personnel Security***
- ***PV – Provenance***
- ***RA – Risk Assessment***
- ***SA – System and Services Acquisition***
- ***SC – System and Communications Protection***
- ***SI - System and Information Integrity***

- ***NIST 800-82 "Guide to Industrial Control Systems (ICS) Security***

R1.2.3 Processes for disclosure of known vulnerabilities:

The guidance document currently states the following: *"Request vendor cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed."*

Vendor release of information concerning **uncorrected** non-public vulnerabilities represents a security threat for the entire industry and is contrary to best practices in the software industry and most vendor's security policies. When a vendor provides such information to a single Responsible Entity, the entire industry is placed at further risk of the information being publically released without a mitigation. There are many industry documents on this topic and as an example OSI strongly urges that SDT review the "Vulnerability Disclosure Framework" documented on the DHS website from the National Infrastructure Advisory Council at the following link:

https://www.dhs.gov/sites/default/files/publications/niac-vulnerability-framework-final-report-01-13-04-508.pdf

The DHS publication states the following as part of its overall recommendations to the President:

"Protect the confidentiality of vulnerabilities for which no known exploitations have been reported while affected vendors are working towards a solution. Coordinate the voluntary disclosure of information regarding exploited vulnerabilities to take into account, among other factors, the risks of damage to the nation's critical infrastructure, the need for completion of ongoing investigations, and the coordinated release of solutions or remedies for the vulnerability."

Some Responsible Entities may believe that they can protect such critical information, but the reality is that their protection is only as strong as their weakest employee clicking on a phishing link. When you consider releasing uncorrected or unmitigated vulnerability details to multiple Responsible Entities of all sizes and levels of security training, the risk of that information falling into the hands of bad actors becomes very high.

OSI therefore strongly urges NERC and the CIP-013 SDT to remove the word "**uncorrected**" from the guidance statement. OSI believes it is critically important to utilize language that does not attempt to compel or otherwise recommend that Responsible Entities request disclosure of uncorrected or unmitigated vulnerabilities from any vendor. OSI will not agree to provide such information and most other vendors will likely adopt the same position. On the other hand, vendors that do agree to these provisions and the entities receiving such information are placing the entire industry at further risk until a mitigation is made available by the vendor – which could be weeks or months after bad actors

become aware of the vulnerability. Responsible vendors will not disclose uncorrected vulnerabilities but will provide recommended mitigations if they are available.

R1.2.5 Processes for verifying software integrity and authenticity of all software and patches that are intended for use:

OSI recommends additional wording in the final paragraph as follows:

When third-party components are provided by the vendor, request vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses ***within a reasonable period that enables the vendor to integrate and complete certification testing of the updated third-party component.***

R1.2.6 Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

OSI recommends additional wording in the 3rd paragraph as follows:

Request vendors maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity. ***The vendor's use of a proxy or intermediate host to provide isolation of connections to Responsible Entity's equipment is one example of best practices for remote access.***

R1.2.7 Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable

OSI recommends additional wording in the 1st paragraph as follows:

Request vendors provide Responsible Entity with audit rights that allow the Responsible Entity or designee to audit vendor's security controls, development and manufacturing controls, access to certifications and audit reports, and other relevant information. ***Responsible Entity review of vendor audit reports completed by industry recognized certification groups can be used as an acceptable method to verify a vendor's security posture. Examples are certified auditor reports for ISO-27001, NIST, etc.***

R4 Part 4.1 Potential Remote Access Controls

Based on the NERC Lessons Learned document at this link (http://www.nerc.com/pa/CI/tpv5impmntnstdy/Vendor%20Access%20Management%20Lesson%20Learned.pdf) , OSI recommends additional wording as follows: ***One acceptable example of best practice is to use a process whereby the remote access session is initiated by the Responsible Entity, and the token code is provided verbally from the Entity to the vendor when requested by the authentication system. This method ensures that the Responsible Entity is in control of the session and the vendor is not allowed access without knowledge of the Entity.***	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	No
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	
Dislikes 0	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	No
Document Name	

Comment
The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”. The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two. The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term. Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included? Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets. Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.” Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”. Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan. Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple places in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, "find another vendor." Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word "mitigate" and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: "mitigating controls to reduce the risk"?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states "The use of controls in planning and development". This line states "applied in procurement and/or operational phase of product or service acquisition and implementation". The "and/or operational" phase is an unnecessary modifier for "product or service acquisition and implementation". It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting "and/or operational phase of".

Page 6, line 1. Provide explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

Page 6., line 5. Notification of all "identified, threatened attempt" is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor's security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

Page 6, line 6: Is the ("Security Event") being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that "have potential adverse impacts to the availability or reliability of BES Cyber Systems" be part of the definition.

Page 6, line 22: For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given. Request clarification as to how this guidance for "requested cooperation" would meet the required "notification".

Page 9 lines 6 and 8: correct numbers "2.2" and "2.3" to be "2.1" and "2.2".

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace “should” with “may”

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

Page 16 line 25, replace “should” with “may”.

The Implementation Plan should more clearly state that contract renegotiation is not necessary during the implementation period if a contract has already begun.

“Vendor” should be a defined term. The Standard should have consistent use of the terms, i.e., only use “vendor” and do not say “third-party.”

Are sub-component manufacturers included under the term “vendor”?

Likes 0	
Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative - 5	

Answer	No
Document Name	
Comment	
Too many changes to the standard to adequately comment on the *Technical Guidance and Examples* document.	
Likes 0	
Dislikes 0	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	No
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	No
Document Name	
Comment	

Based on FE's comments on the Requirements (R1-R5), a detailed review of the Technical Guidance and Examples document is not relevant at this time. However, FE suggests that, in general, it would be helpful if the Technical Guidance and Examples document could provide evidence formats, similar to what is provided in CIP-003-6 Attachment 2.	
Likes 0	
Dislikes 0	
Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	

SRP requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

SRP requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

SRP requests clarification on the term "supplier" as it is used in the guidance document. SRP requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, SRP requests an explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

The Rationale sections of CIP-013 standard and the guidance document use the term "information system". SRP requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced SRP requests that the SDT define the term and place it in the NERC Glossary of Terms.

SRP requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. SRP requests that the following language be added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, SRP requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms. CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities. Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”	
Likes 0	
Dislikes 0	
Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	No
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	

Answer	No
Document Name	
Comment	

Portions of the *Technical Guidance and Examples* document that may affect how the standard is interpreted for audit purposes should be placed in the standard's Guidelines and Technical Basis section and needs to be balloted and approved by industry. As this is not a part of the standard and is not a CMEP Practices Guide, this document should provide implementation guidance in a manner consistent with the NERC Compliance Guidance Policy "to develop examples or approaches to illustrate how registered entities could comply with a standard that are vetted by industry and endorsed by the ERO Enterprise." The implementation guidance is an important item for this standard and Seminole appreciates this work.

As implementation guidance, this document should provide a clear standard manner to address requirements for R1.1 and R1.2.1-R1.2.6, while entities may be able to ask additional questions. While the document discusses ideas of what to include, the biggest value would be to provide an example set of specific questions to vendors on risk management controls. By setting this specification up front, costs drop for both vendors and entities as the vendors can provide the basic set of information in a defined format. Once vendors have a better defined set of expectations, they then know how to meet these expectations across the industry, Further, vendors focused on the electric sector will provide this information, as we are their market. However, we all also use smaller software and hardware vendors that primarily service a broader market, and these smaller vendors would be less willing to provide custom information for separate electric sector entities for a sale amounting to tens or hundreds of dollars.

Open source software does not have a cost or a defined vendor. Risk assessment of open source software should be specifically addressed.

As there is no consistency in the software industry on use of hash functions, guidelines need to be provided on what is considered an acceptable approach to meet this requirement.

This standard essentially eliminates the ability to purchase equipment or services on an emergency basis without a pre-existing contract. This will interfere with incident response and BES recovery operations under extraordinary circumstances.

Likes 0	
Dislikes 0	

W. Dwayne Preston - Austin Energy - 3	
Answer	No
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging. CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.	

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Andrew Gallo - Austin Energy - 6

Answer	No
Document Name	

Comment

AE requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

AE requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

AE requests clarification on the term “supplier” as it is used in the guidance document. AE requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, AE requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. AE requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced AE requests that the SDT define the term and place it in the NERC Glossary of Terms.

AE requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. AE requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, AE requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	

Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	

Likes 0	
Dislikes 0	
Tyson Archie - Platte River Power Authority - 5	
Answer	No
Document Name	
Comment	

PRPA requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

PRPA requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

PRPA requests clarification on the term “supplier” as it is used in the guidance document. PRPA requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, PRPA requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. PRPA requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced PRPA requests that the SDT define the term and place it in the NERC Glossary of Terms.

PRPA requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. PRPA requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, PRPA requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”	
Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

CHPD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

CHPD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CHPD requests clarification on the term “supplier” as it is used in the guidance document. CHPD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CHPD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CHPD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CHPD requests that the SDT define the term and place it in the NERC Glossary of Terms.

CHPD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CHPD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities. Additionally, CHPD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”	
Likes 0	
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	No
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	No
Document Name	
Comment	

As the SDT addresses the comments above regarding the standards, we assume the Technical Guidance and Examples will be modified accordingly.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	No
Document Name	
Comment	
The Guidelines and Technical Basis should include examples to illustrate how implementation is envisioned, and how entities are to be expected to coordinate between SME's and procurement organization, which up to now has not been engaged directly in NERC CIP implementation.	
Likes 0	
Dislikes 0	

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	No
Document Name	
Comment	

More focus should be given to implementation as opposed to justification. I think we all agree with respect to the importance of making sure the Supply Chain is free of malware and although some justification may be necessary to further explain the merits of adding a few additional requirements to the process, overall we are more concerned with implementation strategy. Those implementation methods would better serve us in our own internal controls and for evidence preparation in order to meet the compliance objectives.	
Likes 2	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott; Tallahassee Electric (City of Tallahassee, FL), 5, Webb Karen
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
AEP is concerned about the use of the term “should” in the *Technical Guidance and Examples* document. While AEP understands that the intent of this document is to provide guidance and examples, the use of term “should” may be interpreted by the regional auditors as closer to a mandatory requirement. In order to address this concern, the document could use the term “may” instead. AEP is concerned that this is a shift away from traditional guidelines and technical basis documents, which documents the drafting team’s considerations. The proscriptive nature of this document is concerning when left to the interpretation of different auditors. AEP would not want this document to become akin to an actual Requirement without going through the proper process.	
Likes 0	
Dislikes 0	

Marty Hostler - Northern California Power Agency - 5	
Answer	No
Document Name	
Comment	
See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	No
Document Name	
Comment	
The statement on p.1 that CIP-013-1, “does not require the Responsible Entity to renegotiate or abrogate existing contracts,” implies that no action needs to be taken for existing PEDs. This point should be made explicit in the standard per se, but our “additional comments” concerns would still apply for replacing or upgrading existing equipment. The Technical Guidance and Examples document should be revised to address our negative-ballot comments. Our concerns regarding willingness and ability of vendors to be CIP-013-friendly appear to already be at least partly recognized, ref. for example the statement on p.3, “Obtaining the desired specific cyber security controls in the negotiated contract may not be feasible with each vendor.” The subsequent comment that “every negotiated contract will be different,” indicates however that we and the SDT are not on common ground regarding practicality.	
Likes 0	

Dislikes 0	

faranak sarbaz - Los Angeles Department of Water and Power - 1	
Answer	No
Document Name	
Comment	
The standard as written doesn't clearly address the objectives as listed in its Requirements. It also creates confusion and possible double jeopardy with other CIP Standards.	
Likes 0	
Dislikes 0	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
Although NERC's Compliance Guidance Policy document describes certain procedures by which a drafting team may provide Compliance Guidance, ERCOT suggests that it is generally preferable to provide examples of acceptable conduct in the standard itself, rather than in an ancillary document, which Responsible Entities would have to remember and separately locate and review. The team could achieve this purpose by using language in the standard such as: "Practices that comply with this requirement include, without limitation, the following: . . . ." ERCOT notes that in a number of instances, the draft Technical Guidance and Examples document uses normative language (e.g., "should"), rather than permissive (e.g., "may") language, which suggests that the Technical Guidance document is instead intended to serve	

simply as a more detailed set of requirements, as opposed to describing one of potentially many acceptable methods of achieving compliance. For example, the guidance for R1 states: "In implementing Requirement R1, the responsible entity should consider the following: . . . ." To the extent the drafting team intends the guidance in this document to be followed, it should be included in the standard.	
Likes 0	
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.	
Likes 0	
Dislikes 0	
Pablo Onate - El Paso Electric Company - 1	
Answer	No
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	No
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot on this item.	
Likes 0	
Dislikes 0	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	

Due to the early stage of development of this standard, NRECA is not able to support specific Technical Guidance and Examples.	
Likes 0	
Dislikes 0	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	No
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	No
Document Name	
Comment	

Oxy does not agree with the proposed language of the requirements and therefore cannot agree with the *Technical Guidance and Examples* document until requirements are revised and updated and corresponding updates are made to the *Technical Guidance and Examples* document.	
Likes 0	
Dislikes 0	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	No
Document Name	
Comment	
Without being able to evaluate the Technical Guidance and Examples document against the eventual final Standard, the company cannot offer its support.	
Likes 0	
Dislikes 0	
Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	

Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	No
Document Name	
Comment	
The Technical Guidance Document is well-written based upon what the NERC Drafting Team had to work with, but the controls recommendations are expansive enough to become its own industry. This would be an excellent document to use as a starting point of conversation with our hardware and software supply chain, but to impose it on the Entities as the end customers of these ICS products and applications would be overly burdensome with very little return on investment. This would be particularly true for those Entities dealing only with Low Impact BCS.	
Likes 0	
Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	No
Document Name	

Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	No
Document Name	
Comment	

1) The guidance document is suggestions or recommendations. Request replacing all imperative language such as “should” with discretionally language such as “may”.

2) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

3) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or define the term.

4) Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

5) Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

6) Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

7) Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

8) Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

9) Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

10) Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

11) Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

12) Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

13) Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

14) Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

15) Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

16) Page 6., line 5. Notification of all “identified, threatened attempt” is too broad for large and highly visible vendors like Microsoft. The scope should be limited to only the identified, successful breaches in the vendor’s security that the vendor determines could have impact on the entities equipment or services associated with BES Cyber Systems.

17) Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be a NERC Glossary term. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition.

18) Page 6, line 22: For R1.2.2: The requirement for the ”process for notification” is very different than the “request vendor cooperation” guidance given. Request clarification as to how this guidance for “requested cooperation” would meet the required “notification”.

19) Page 9 lines 6 and 8: correct numbers “2.2” and “2.3” to be “2.1” and “2.2”.

20) Page 11, Line 15, replace supplier with Vendor.

21) Page 11, line 25, replace “should” with “may”

22) Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

23) Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

24) Page 12 line 33. Provide additional clarity on “monitor”. Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

25) Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

26) Page 15, line 23 Provide guidance on the meaning of “timely manner.” Would responding to an issue discovered in a 30-day log review be considered timely? How does “timely manner” align with “during the remote access session” language of R4.3.

27) Page 16 line 25, replace “should” with “may”.

Likes 0	

Dislikes 0	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	No
Document Name	
Comment	
Avista supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	No
Document Name	
Comment	
Requirement R1 needs to be vendor focused. It is not appropriate to assign risk based on the categorization of BES Cyber System impacted by the procurement. This Standard is for supply chain management, not BES Cyber System management. The guidance should not be limited to a brief discussion of Black Energy. To the contrary, the risks presented by Havex appear to be the stronger driver of need as perceived by FERC. It is imperative that vendor risk management controls, such as those cited on Page 4, starting at Line 13, comport with the substantively same or similar requirements of other CIP Standards before being allowed. The Guidance should also address the situation where the Registered Entity has chosen a patch source, per CIP-007-6, Requirement R2, that is not the originator of the software. For	

example, where the Registered Entity chooses to get its Microsoft and Linux patches from its SCADA/EMS vendor. Some sort of integrity chain needs to be verified.	
Likes 0	
Dislikes 0	
Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	No
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
The Technical Guidance Document is well-written based upon what the NERC Drafting Team had to work with, but the controls recommendations within this document are expansive enough to become its own industry. This would be an excellent document to use as a starting point of conversation with our hardware and software supply chain, but to impose it on the Entities as the end customers of these ICS	

products and applications would be overly burdensome with very little return on investment. This would be particularly true for those Entities dealing only with Low Impact BCS.	
Likes 0	
Dislikes 0	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	No
Document Name	
Comment	
GTC recommends the SDT consider GTC's comments above, and adapting the Technical Guidance and Examples document accordingly.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	

Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.	
Likes 0	
Dislikes 0	
Terry BIlke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	No
Document Name	
Comment	
R1: The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an existing contract? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard or in the implementation plan. Please clarify how existing versus new procurement elements are addressed, especially for R3 and R4 technical controls.	
Likes 0	
Dislikes 0	
William Wenz - AES - Dayton Power and Light Co. - NA - Not Applicable - RF	

Answer	No
Document Name	
Comment	
Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.	
Likes 0	
Dislikes 0	

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	
Comment	
As the *Technical Guidance and Examples* is not legally enforceable LCRA cannot rely on it as an authoritative source for guidance on complying with CIP-013.	
Likes 0	
Dislikes 0	

Jeff Johnson - Sempra - San Diego Gas and Electric - 1,2,3,4,5,6,7 - WECC

Answer	No

Document Name	
Comment	
SDG&E agrees with EEI comments and proposed language.	
Likes 0	
Dislikes 0	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	No
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

Some of the Technical Guidance and Examples reads more like implementation guidance and other parts sound more like Guidelines and Technical Basis, which should be worked out before industry can adequately provide comments. Also, due to our concerns with the requirements, this document will need to change as well.	
Likes 0	
Dislikes 0	

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	No
Document Name	

Comment

SMUD requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

SMUD requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

SMUD requests clarification on the term “supplier” as it is used in the guidance document. SMUD requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, SMUD requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. SMUD requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced SMUD requests that the SDT define the term and place it in the NERC Glossary of Terms. SMUD requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. SMUD requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities. Additionally, SMUD requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”	
Likes 0	
Dislikes 0	
Erick Barrios - New York Power Authority - 5	
Answer	No
Document Name	
Comment	
The NYPA Comments	
Likes 0	
Dislikes 0	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA	
Answer	No
Document Name	
Comment	
FMPA agrees with comments submitted by American Public Power Association.	
Likes 0	
Dislikes 0	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	No
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	
Comment	

Seattle City Light requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging.

Seattle City Light requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

Seattle City Light requests clarification on the term "supplier" as it is used in the guidance document. Seattle City Light requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, Seattle City Light requests an explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

The Rationale sections of CIP-013 standard and the guidance document use the term "information system". Seattle City Light requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced Seattle City Light requests that the SDT define the term and place it in the NERC Glossary of Terms.

Seattle City Light requests that the SDT consider defining the term "Security Event" (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. Seattle City Light requests that the following language added to the definition "have potential adverse impacts to the availability or reliability of BES Cyber Systems" and that the entities be required to report only newly identified security vulnerabilities.

Additionally, Seattle City Light requests that the SDT define the term "vendor security event" or replace it with "identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System."

Likes 0	
Dislikes 0	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	No
Document Name	
Comment	

R1: The Compliance Guidance states: “Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P 36) as specified in the Implementation Plan.” What qualifies as an existing contract? Is there an obligation to implement the risk management plan when: (1) negotiating and executing a new Statement of Work; (2) negotiating an amendment to a Master Agreement; or (3) renewing a contract under existing terms? The answer to these questions should be clarified and directly addressed in the standard or in the implementation plan.

Please clarify how existing versus new procurement elements are addressed, especially for R3 and R4 technical controls.

Likes 0	
Dislikes 0	

Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	No
Document Name	
Comment	

CSU requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging.

CSU requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

CSU requests clarification on the term “supplier” as it is used in the guidance document. CSU requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, CSU requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. CSU requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced CSU requests that the SDT define the term and place it in the NERC Glossary of Terms.

Colorado Springs Utilities (CSU) requests that the SDT consider defining the term “Security Event” (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. CSU requests that the following language added to the definition “have potential adverse impacts to the availability or reliability of BES Cyber Systems” and that the entities be required to report only newly identified security vulnerabilities.

Additionally, CSU requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Nathan Mitchell - American Public Power Association - 3,4	
Answer	No
Document Name	
Comment	

1) The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

2) The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or, define the term.

3) Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

4) Page 6, line 6: Is the (“Security Event”) being used to define a term that is used not only in this document but in R1.2.1? If so, it should be either defined in this standard or in the NERC Glossary of Terms. If the term is defined by the language here, recommend that ”have potential adverse impacts to the availability or reliability of BES Cyber Systems“ be part of the definition. The “threatened, attempted” part of this definition would is too large in scope and could require large vendors like Microsoft or Cisco to report thousands or millions of attempts each day. Suggest replacing “vendor security event” in R1.2.1 with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

5) Page 6, line 12: It is unclear that the R1.2.1 requires notification by the entity to the vendor.

6) Suggest adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

7) In other standards, the Guidelines and Technical Basis document is included in the standard, suggest that this also be completed for CIP-013.

Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No

Document Name	
Comment	
BPA proposes the “Supply Chain” requirements should be clear on what is to be done during the procurement process. Any aspects of service or ongoing maintenance activities should be addressed in the appropriate CIP standard. All requirements for Low impact systems should be in CIP-003.	
Likes 0	
Dislikes 0	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	No
Document Name	
Comment	
As the *Technical Guidance and Examples* is not legally enforceable, LCRA cannot rely on it as an authoritative source for guidance on complying with CIP-013.	
Likes 0	
Dislikes 0	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	No
Document Name	

Comment
Santee Cooper suggests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper-proof packaging. Santee Cooper requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards. Santee Cooper requests clarification on the term “supplier” as it is used in the guidance document. Santee Cooper suggest using consistent terms between the standard and the Technical Guidance. In the guidance document on page 6, line 1, Santee Cooper requests an explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.” The Rationale sections of CIP-013 standard and the guidance document use the term “information system”. Santee Cooper requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. Additionally, Santee Cooper requests that the SDT define the term “vendor security event” or replace it with “identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System.”

Likes 0	
Dislikes 0	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

The Technical Guidance and Example language states, “Entity processes for addressing software risks and vendor remote access risks per Requirements R3 and R4. Consider whether to include low impact BES Cyber Systems in these processes, or alternatively develop a separate cyber security policy or process(es) to address low impact BES Cyber Systems.” R5 states that Responsible Entities must have “one or more documented cyber security policies.” IPC would like to know why the Technical Guidance and Examples language directs Responsible Entities to consider developing “processes” to meet a requirement that explicitly states that Responsible Entities must have “one or more documents cyber security policies” to meet the requirement?	
Likes 0	
Dislikes 0	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Though each of the objectives in Order 829 is addressed, Reclamation recommends a more simplified format for the requirements as the SDT originally suggested in the webinar on November 10, 2016. The entire standard addresses supply chain risk management and therefore should address the possible risks and possible controls for entities to consider for each stage of the life cycle of a system in which there is interaction with and dependence on vendors, their products, and/or their services. These may include but are not limited to evaluation of design, procurement, acquisition, testing, deployment, operation, and maintenance. Reclamation recommends the technical guidance document provide examples of risks and their respective controls (such as contract clauses) for entities to consider.	
Likes 0	
Dislikes 0	

Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	No
Document Name	
Comment	
1. Please include guidance on expectations for resource and time to support the requirements. Most low impact entities do not have a procurement office or manager and are wondering who should be hired or trained to support the supply chain issues.	
Likes 0	
Dislikes 0	
Amy Casuscelli - Amy Casuscelli On Behalf of: David Lemmons, Xcel Energy, Inc., 5, 3, 1; - Amy Casuscelli	
Answer	No
Document Name	
Comment	
Xcel Energy supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Brian Bartos - CPS Energy - 1,3,5	
Answer	No
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Lauren Price - American Transmission Company, LLC - 1	
Answer	No
Document Name	
Comment	
This document identifies some shortcomings, pitfalls, and/or unintended consequences of prescribing requirements within a mandatory reliability standard and is evidence that a Reliability Standard may not be the best vehicle to address the complexities and broad range of individual Registered Entity nuances in process and infrastructure, on top of the host of jurisdictional, technical, economic, and business relationship issues associated to supply chain; and further demonstrates the essentiality of reconsidering the need for CIP-013-1.	
Likes 0	
Dislikes 0	
Ballard Mutters - Orlando Utilities Commission - 3	

Answer	No
Document Name	
Comment	

OUC requests adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging.

OUC requests that the Technical Guidance and Examples be included in the standard consistent with the other CIP standards.

OUC requests clarification on the term "supplier" as it is used in the guidance document. OUC requests replacing with the term vendor or providing clarification on the difference between the two.

In the guidance document on page 6, line 1, OUC requests an explanation on how the term "vendor" used in the requirements relates to "supplier's system component, system integrators, or external service providers."

The Rationale sections of CIP-013 standard and the guidance document use the term "information system". OUC requests replacing this with the appropriate NERC defined term: BES Cyber System, Cyber Asset. If the term cannot be replaced OUC requests that the SDT define the term and place it in the NERC Glossary of Terms.

OUC requests that the SDT consider defining the term "Security Event" (page 6, line 6 and R1.2.1) and placing it in the NERC Glossary of Terms. OUC requests that the following language added to the definition "have potential adverse impacts to the availability or reliability of BES Cyber Systems" and that the entities be required to report only newly identified security vulnerabilities.

Additionally, OUC requests that the SDT define the term "vendor security event" or replace it with "identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System."

Likes 0	
Dislikes 0	

Si Truc Phan - Hydro-Qu?bec TransEnergie - 1 - NPCC	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	

Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	

(Page 2, lines 2-3) An entity should define its specific approach to the SCRM plan in the preamble, so the Regional Entity will be able to evaluate the development and application of the plan.

(Page 2, lines 16-24: This passage gives entities a huge pass on implementation. As long as the entity asked the vendor to play nice during the RFP process, it appears the entity may not be found in noncomoliance if the final vendor contract does not include part or all of the entity's SCRM RFP clauses. This means it will be important to evaluate both the RFP and the final Service Level Agreement [SLA]/Contract for a specific

applicable BCS. This review may lead to Recommendations and/or Areas of Concern [AoC], but might be difficult to substantiate Possible Non-Compliance [PNC] Finding as long as the RFP process aligns with the entity's SCRM plan.

(Page 2, line 37). This is true only if such actions are specified in the vendor's SLA.

(Page 3, lines 9-10). This was discussed on an earlier SCRM SDT call, if a vendor can demonstrate that it is certified by ISO or some other certification organization, it may provide a statement to that effect, in lieu of specific agreements with each customer. This issue may still be fluid, but should be included in the final Guidance, as well, in order to satisfy FERC's directive to not extend CIP-013-1 beyond the purview of Section 215 to vendors.

(Page 3, lines 29-30). It appears the key element in this passage is to ensure entities have implemented a sound SCRM program and suitable processes to mitigate vendor risk, it does not require entities to take extraordinary measures to ensure all such processes are included in final SLAs.

(Page 3, lines 42-44) We can reasonably expect most, if not all, SCRM plans to follow the guidelines below to incorporate applicable controls into the plan. However, these suggested controls are best practices, but not mandatory controls. Entities can use these guidelines as an initial starting point for the development of the SCRM plan, as can the Regional Entities for review and evaluation of the R1 SCRM plan at audit..

(Page 4, footnote 1). This footnote cites a third party commercial product. WECC's approach to maintaining auditor independence includes its position to never endorse, recommend, or otherwise indicate favorite vendor status to any consultant, vendor, or product. As a result of this approach, WECC does not consider it appropriate to recommend or endorse a specific tool such as this product.

(Page 5, lines 34-37). This bullet addresses the potential for contractual controls for SCRM that stems from a sound RFP process and procedures. If an entity takes this approach, WECC would expect to see an RFP template that includes specific cyber security terms and expectations. We would then sample for completed RFPs to evaluate the entity's implementation of this approach.

(Page 6, Section 1.2.1 line 4). Unless these processes are specifically included in a vendor SLA or other binding document, it will be difficult for a Regional Entity to evaluate anything other than the entity's plan for such notifications. Since the burden of proof cannot be passed along to the vendor other than through contract, the audit of most of these 1.2.x sections may generally be nothing more than a review of the entity's plan.

(Page 10, lines 6-7). Communications and training materials relative to SCRM should also be addressed in the entity's overall Cyber Security Awareness program. (Page 13, R4). As mentioned in the R4 comments above, this is a major security concern from WECC's perspective and should leverage and expand upon an entity's controls and procedures for Interactive Remote Access [IRA] from CIP-005-5 R2. (Page 16, R5). An entity can leverage its R3 and R4 controls to support R5, but it is not required to do so. However. based on prior discussions with entities relative to CIP-010-2 R4, in practice, WECC would expect to see implementation efforts of this nature relative to SCRM controls for Low-impact BCS.	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	Yes

Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Currently, implementation guidance is imbedded in the Technical Guidance document covering what the Standard means, and how to implement it. Southern requests that those topics be separated out.	
Likes 0	
Dislikes 0	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	Yes
Document Name	

Comment

PSEG appreciates the standard drafting team's effort in providing technical guidance and examples to provide additional clarity and implementation support for the registered entities. PSEG has the following questions/recommendations to the Technical Guidance and Examples document below:

- The term vendors as used in the standards is defined (Page iv Line 6) in the Technical Guidance and Examples document (as well as in the Rationale for Requirement R1 in the draft CIP-013 Standard). This term should be officially defined in the Glossary of Terms used in NERC Reliability Standards.

- Page 4, line 37: Add the wording "as determined by the Registered Entity" after the word components. The new statement would state, "Define any critical elements or components, as determined by the Registered Entity, that may impact the operations or reliability of BES Cyber Systems". This change aligns with the FERC order (p31) statement that the standard should have flexibility to account for varying " differences in the needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risks" to determine the critical elements and components that may impact operations or reliability of BES Cyber systems based on the registered entities implementation of a vendor system or component within their program.

- Page 5, line 24: Add the wording "as identified by the Registered Entity" after the word "risks". The new statement would state, "Review and address other risks as identified by the Registered Entity in Requirement R1 Part 1.1.1." Recommend this change to align with the change to technical guidance for Requirement 1.1.1 (Page 4, line 37) above.

- Page 6, line 43: Replace the word "breaches" with "vulnerabilities and threats" to align with the use of the word "vulnerabities" in the requirement language.

- Page 7, line 1: Replace the word "breach" with "vulnerability" to align with the use of the word "vulnerabities" in the requirement language.

- Page 7, line 9: Remove the words "availability or". The NERC CIP reliability standards require protecting BES Cyber Systems to support reliable operation of the BES. Recommend removing availability to align with the wording used throughout the NERC CIP reliability standards.

• Page 13, line 9: Recommend changing Requirement 4.3, from “Disabling or otherwise responding to unauthorized activity during remote access sessions“to “Disabling or otherwise responding to detected unauthorized activity associated with remote access sessions.” (see comment under question 4) • Page 15, line 22: Recommend adding the word “detected” to align with the recommended changes to Requirement 4.3. The statement would become “Set up alerting and response processes so that detected inappropriate vendor remote access sessions may be disabled or otherwise responded to in a timely manner. • Page 15, line 23: The words “in a timely manner” are overly subjective. Recommend specifying a specific time frame for a timely response.	
Likes 1	PSEG - Public Service Electric and Gas Co., 3, Mueller Jeffrey
Dislikes 0	
Stephanie Little - APS - Arizona Public Service Co. - 5	
Answer	Yes
Document Name	
Comment	
AZPS requests clarification that the Technical Guidance and Examples being incorporated into the Standard will be used as technical guidance only, and not compliance guidance.	
Likes 0	
Dislikes 0	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Mike Smith - Manitoba Hydro - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Tom Anthony - Florida Keys Electric Cooperative Assoc. - 1,3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Dennis Minton - Florida Keys Electric Cooperative Assoc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	

Document Name	
Comment	
There is inconsistency with the language of the Requirements and the Technical Guidance language, specifically in reference to Requirement R3 and Requirement R4. The guidance sections for both Requirements mention reviewing security policies, however, the Requirements mention Risk Management Plans. NRG suggests that this language be properly aligned or else this could lead to future Compliance Enforcement issues for the industry. NRG requests SDT clarity that system-to-system is equivalent to machine-machine.	
Likes 0	
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
On Page 9, line 43, the Technical Guidance and Examples references the use of industry best practices and guidance that improve cyber security risk management controls. This does not match the rationale of R2 which only speaks to the use of guidance. Exelon feels that the reference to “industry best practices” should be removed from the Technical Guidance and Examples since it is non-specific and open to interpretation.	
Likes 0	
Dislikes 0	

Kenya Streeter - Edison International - Southern California Edison Company - 6	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	

The term “supplier” is used in the guidance document. Recommend replacing with Vendor or providing clarification on the difference between the two.

The Rational sections of CIP-013 standard and the guidance document uses the term “information system”. Recommend replace this with the appropriate NERC defined term: BES Cyber System, Cyber Asset…. Or, define the term.

Vendor should be a defined term. Suppliers should also be defined. Also, need consistent use of vendor vs third-party. Are sub-component manufacturers included?

Page 1, line 37 that starts with “These cyber system cover the scope of assets needed….” to “These Cyber Assets cover the scope needed …” The term “assets” is not defined by NERC but is used in CIP-003 to identify substations and generation assets.

Page 2, line 23. The sentence “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” should be changed to “Obtaining specific controls in the negotiated contract may not be feasible. In these cases, failure to obtain and implement these controls is not considered a failure to implement an entity's plan.”

Page 2, line 32: change “cited to the BlackEnergy” to “Cited the BlackEnergy”.

Page 2, line 46: Change this line to be “In the development of the supply chain risk management plan, the responsible entity may consider the following:”. It seems like the bullets listed on page 8 seem to be considered in the development of the supply chain risk management plan and not in the implementation of the plan

Page 3: The format that NERC uses for writing standards is that bulleted items are “or” clauses. These bullets should be numbered and not bullets. This is an issue in multiple place in this document.

Page 3, line 24: This paragraph is not consistent with the SDT response given during the 2/2/17 webinar when asked what a responsible entity should do when a vendor will not or cannot agree to controls required by this standard. The SDT said, “find another vendor.” Request that the SDT clarify a consistent answer.

Page 3, line 32: Please provide clarity to the meaning of the word “mitigate” and the possible expectation that all risks can be mitigated 100%. Would the phrase used on line 39 be better: “mitigating controls to reduce the risk”?

Page 4, line 29: The System Development Life Cycle program (SDLC) seems like a defined program. Provide reference to the standard, document or agency that can give details on this.

Page 5, line 14: *determine mitigating controls* implies implementation, which is different than the requirement to *evaluate methods*

Page 5, line 14: R 1.1 states “The use of controls in planning and development”. This line states “applied in procurement and/or operational phase of product or service acquisition and implementation”. The “and/or operational” phase is an unnecessary modifier for “product or service acquisition and implementation”. It could be interpreted to extend the scope beyond the planning and development cycles. Recommend deleting “and/or operational phase of”.

Page 6, line 1. Provide explanation on how the term “vendor” used in the requirements relates to “supplier’s system component, system integrators, or external service providers.”

Page 6, line 6: Is the ("Security Event") being used to define a term that is used not only in this document but in R1.2.1? If so, it should be either defined in this standard or in the NERC Glossary of Terms. If the term is defined by the language here, recommend that "have potential adverse impacts to the availability or reliability of BES Cyber Systems" be part of the definition. The "threatened, attempted" part of this definition would is too large in scope and could require large vendors like Microsoft or Cisco to report thousands or millions of attempts each day. Suggest replacing "vendor security event" in R1.2.1 with "identification of a new security vulnerability that could have potential adverse impact to the availability or reliability of BES Cyber System."

Page 6, line 12: It is unclear that the R1.2.1 requires notification by the entity to the vendor.

Page 6, line 22: For R1.2.2: The requirement for the "process for notification" is very different than the "request vendor cooperation" guidance given. Request clarification as to how this guidance for "requested cooperation" would meet the required "notification".

Page 9 lines 6 and 8: correct numbers "2.2" and "2.3" to be "2.1" and "2.2".

Page 11, Line 15, replace supplier with Vendor.

Page 11, line 25, replace "should" with "may"

Page 12, line 3-9 italicize to be consistent with other areas of this guidance when the Requirements are quoted.

Page 12 line 13. Provide clarity that system-to-system is equivalent to machine-machine.

Page 12 line 33. Provide additional clarity on "monitor". Is reviewing logs considered monitoring or is this actively viewing the actions being performed through the remote access session? If it is the latter, how would this be done on a system-to-system remote access session?

Page 14, line 15 Monitoring and logging are listed as separate items in both the guidance and the Standard. Request guidance on the use of logging as a monitoring activity.

Page 15, line 23 Provide guidance on the meaning of "timely manner." Would responding to an issue discovered in a 30-day log review be considered timely? How does "timely manner" align with "during the remote access session" language of R4.3.

Page 16 line 25, replace "should" with "may".

Suggest adding possible logical controls in addition to the physical controls listed on Page 12, 4th bullet under both software integrity and authenticity controls. This bullet lists only physical controls such as tamper proof packaging In other standards, the Guidelines and Technical Basis document is included in the standard, suggest that this also be completed for CIP-013.	
Likes 0	
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE has no comments for this question.	
Likes 0	
Dislikes 0	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	
We did review the TG&E document briefly and it was valuable in illustrating how some of the team members were viewing various requirements; however, it will need to be further refined once the changes are made to the requirements. We did note that in the discussion of integrity and authenticity, there was a lot of duplication in methods between the two making it seem that there might be some fuzziness on what each of the two descriptors are trying to address.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	
Document Name	
Comment	

- See APPA's comments.	
Likes 0	
Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	
Glenn Pressler - CPS Energy - 1	
Answer	
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	

Dislikes 0	

9. Provide any additional comments for the SDT to consider, if desired.

Summary Consideration. The SDT thanks all commenters. The SDT made significant revisions to proposed CIP-013-1 and developed revisions to other CIP standards as suggested by stakeholders. The SDT believes these changes are responsive to stakeholder feedback and meet the reliability objectives in the Project 2016-03 Standards Authorization Request (SAR) that was accepted by the Standards Committee in January 2017. Some stakeholders commented on issues that are beyond the scope of Order No. 829 and the Project 2016-03 SAR. The SDT is not proposing revisions that are outside of the established project scope or that the SDT believes would not meet the project objectives.

Russel Mountjoy - Midwest Reliability Organization - 10	
Answer	
Document Name	
Comment	

In voting “no” on this proposed Reliability Standard, MRO acknowledges the impossible challenge faced by the Standard Drafting Team and NERC in developing a Supply Chain Reliability Standard as directed in FERC Order No. 829 issued July 21, 2016. Federal Energy Regulatory Commission (FERC) Acting Chairman LaFleur (then a commissioner), stated in her dissenting opinion, “[E]ffectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, economic, and business relationship issues.”

As a regulator, MRO seeks to provide clarity about Reliability Standard requirements, assurance around compliance with those Reliability Standards, and results – reduced risk to the reliable operation of the bulk power system (BPS). Adoption of the proposed Reliability Standard will not meet these goals.

The proposed Reliability Standard directs registered entities to complete tasks that require agreement of vendors that are not subject to the jurisdiction of the FERC or the Electric Reliability Organization (ERO). To accommodate this lack of jurisdiction, the proposed Reliability Standard is drafted sufficiently vague to allow for lack of vendor agreement and compliance with the Reliability Standard to exist at the same time. For example, Requirement 1 of CIP-013 obligates registered entities to implement supply chain risk management plans. At the same time, the supporting Rationale states, “obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement the entity’s plan.” In essence, this Requirement forces entities to develop a plan, but a failure to be able to implement the plan

is not an issue of noncompliance. The root cause of the problem is that the risk lies with vendors, a third party not subject to FERC or ERO jurisdiction. Thus, the Reliability Standard becomes more paperwork and administrivia than mitigation of risk. See the comments of the MRO stakeholder-driven NERC Standards Review Forum.

As a regulator, MRO believes the proposed Reliability Standard cannot be effectively and efficiently assessed and therefore MRO would not be able to provide assurance of compliance or, more important, assurance of reduced risk to the reliable operation of the BPS. As drafted, MRO will be expected to determine if registered entities made a reasonable attempt to address supply chain risks through their procurement processes. Since contracts are always a give and take with regard to a number of provisions, how does a regulator efficiently and effectively monitor one aspect of the contract negotiation process to determine reasonableness and the possible existence of countermeasures to address security throughout the procurement process which may be beyond our jurisdiction and rest with best security practices?

In addition, the draft Reliability Standard does not address supply chain management comprehensively. For example, the issues associated with vendors of the vendors are not addressed. It is very common for an Energy Management System (EMS) vendor to deliver a system with third party software, such as Adobe®, Java, or even open-sourced software such as PuTTY. The vendor chain for any system can be deep and the proposed Reliability Standard does not provide registered entities clarity on how to deal with these routine layers of vendors.

Finally, it is also important to consider the potential economic impact on future contract negotiations between registered entities and vendors. The proposed CIP-013 directs a registered entity to address supply chain risks in its vendor contracts. How much does the registered entity pay to manage supply chain risk when the vendor has no legal obligation to accommodate the registered entity? By placing additional requirements on vendors, do we unintentionally reduce competition, increase costs, and reduce innovation? Furhtermore, the possibility of less competition, creates less diversity across the bulk power system and less diversity increases risk.

Reducing supply chain risk to the reliable operations of the BPS and providing the requisite regulatory assurance that that risk has been reduced is a complex task for the very reasons FERC Acting Chairman LaFleur communicated in her dissent. Whether or not this risk is best addressed by a NERC Reliability Standard as opposed to a security framework, an IEEE standard or use of military grade components merits greater consideration. This is particularly true given four of the five FERC commissioners will have either not considered or not supported FERC Order 829 when the proposed Reliability Standard is ultimately filed with FERC. Following the comment period, MRO recommends that FERC and the ERO consider whether we have the appropriate structure and expertise to address and mitigate this risk that resides with vendors effectively and efficiently through a Reliability Standard.

Likes 2	Platte River Power Authority, 5, Archie Tyson; Gresham Darnez On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1,
Dislikes 0	

Joseph DePoorter - MGE Energy - Madison Gas and Electric Co. - 4, Group Name MRO NSRF	
Answer	
Document Name	
Comment	

The NSRF has concerns with being held accountable for a vendor who does not meet the attributes of this proposed Standard, especially for entities that have Low Impact BES Cyber Systems, only. Many of the entities that have Low Impact BES Cyber Systems only, are small (read low risk) entities that may have one Low Impact BES Cyber Systems (maybe a generator, one Transmission substation, or control system). How is the small entity going to stand up to large multi-regional corporate companies (i.e. the vendor), when the vendor will not comply with the requirements of the small entity (and CIP-013-1)? The Low Impact BES Cyber Systems entity will carry all the compliance risks (burden) when they find out that the vendor did not comply with said requirements, regardless of how the entity will ensure that the vendor will comply, a contract, statement of work, etc. If the vendor does agree with supplying proof that is requested, the small entity will then incur **more cost** (read increase costs) to the Low Impact BES Cyber Systems entity by being found non-compliant. The entity may not be able to recoup that cost due to the rate structure of that entity's state commission. This may lead the small entity to assume more risks because the cost is too great and not have a system fully protected. They would be fully compliant by writing their plan and stating everything is low risk and controls are not required.

The guidance document suggests not making these requirements contractual language as it makes negotiations more difficult. This puts us in a poor situation as we are required to do it but don't get NERC support via a requirement in the standard to force the agreement to stipulate it. If it was part of the standard to require it, it would give all Responsible Entities consistent leverage to utilize as all would require it. NERC should provide the areas that should be covered in an agreement in a standard format to provide consistency. The Standard does not make it

clear how any cloud based services may be impacted by this standard. We suggest the SDT to consider how this standard may apply to cloud based systems and provide any relevant clarifications.	
Likes 2	Platte River Power Authority, 5, Archie Tyson; OTP - Otter Tail Power Company, 5, Fogale Cathy
Dislikes 0	
Karie Barczak - DTE Energy - Detroit Edison Company - 3, Group Name DTE Energy - DTE Electric	
Answer	
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Donald Lock - Talen Generation, LLC - 5	
Answer	
Document Name	
Comment	
We are concerned that CIP-013-1 may oblige entities to purchase equipment that doesn't presently exist and may never exist, and to take actions that are impossible. The standard should at a minimum state that it does not require NERC entities to:	

- impose cyber security measures or reporting on the suppliers of programmable electronic devices (PEDs), - monitor vendors to ensure that they are properly implementing their cyber security programs, - ensure that as-received software and firmware is in the as-shipped condition. - eliminate risk (only mitigation of risk is possible). It would be impractical for vendors to individually negotiate a unique CIP agreement with each purchaser, and the net effect on BES reliability could be negative if the current vendor (for NERC entities with standardization programs) or the vendor with the best product (for competitive bidding) chooses not to develop CIP-013-friendly products due to the burden of compliance. We would support a qualification program administered by a NERC-approved central authority, however, such that entities could address supplier-related issues simply by purchasing CIP-013-certified products. A blanket allowance is needed for entities to take technical feasibility exceptions (TFEs), to address the wide variety of PED types and to address instances of vendors not producing the inputs that entities are supposed to act upon. CIP-013-1 as presently written may create extreme reluctance to enhance plants in accordance with technological developments, which again would be counterproductive regarding long-term BES reliability.

Likes 0	
Dislikes 0	
Marty Hostler - Northern California Power Agency - 5	
Answer	
Document Name	
Comment	

See APPA's, TAP's, and USI's comments.	
Likes 0	
Dislikes 0	
Thomas Foltz - AEP - 5	
Answer	
Document Name	
Comment	
AEP believes the SDT should specifically mention CIP Exceptional Circumstances in the Standard in order to clearly identify that entities would be exempt from complying with CIP-013-1 in the event of a qualifying CIP Exceptional Circumstance. In addition, Order 829 specifically mentions that the Standard should be forward-looking, but CIP-013-1 does not mention it. AEP believes the SDT should revise CIP-013-1 to include a statement in alignment with FERC's directive that this Standard should be forward-looking.	
Likes 0	
Dislikes 0	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	
Document Name	
Comment	

Please modify this standard using the similar 'Applicability' table format used in the earlier standards.

This set of base requirements is would duplicate effort on the part of each entity to evaluate Supply Chain risk for vendors that provide the same product to multiple entities. Some consideration should be given to creating a standard review, application or qualification form that vendors can complete to certify their product and its delivery.

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority

Answer	
Document Name	

Comment

There is significant overlap to CIP-005, 007, 008, 010. If the intent is to impose additional requirements on the procurement process those requirements should be integrated into the appropriate standard to maintain the linkage. Duplication of requirements in another standard will only create confusion and wasted effort for entities to meet CIP compliance.

The requirements as written are not consistent with the standard's stated purpose: "To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems." This purpose statement indicates this standard is intended to address items that should be considered during the procurement/contract negotiations process and included in terms of the contracts. The requirements as written imply that enforcement of the terms of the contract will be audited. The lifecycle management is currently addressed in CIP-005, 007, 008, 010.

The applicability of each of the requirements is not clearly addressed. Standards CIP-002 through CIP-011 clearly define the applicability for each requirement and sub-requirement.

2. Suggest include supply chain certifications such as ISO-28000 and Customs-Trade Partnership Against Terrorism certification as items to ask for in request for purchase.	
Likes 0	
Dislikes 0	
Romel Aquino - Edison International - Southern California Edison Company - 3	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Shelby Wade - PPL NERC Registered Affiliates - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	
Document Name	
Comment	
R1.2.6 states the RE needs to provide	

"*Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s);"* While R4 and R5 require *"Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s)."* Different terms regarding obligations for vendor remote access have been used with regard to R1.2.6 than under R4 and R5 (e.g., "coordination" and "controlling:"). We seek clarification on whether that is intentional. If the two terms are intentionally different, more clarity is needed on what different obligations are being imposed between R1.2.6 and R4/R5. If R1.2.6 and R4/5 are not meant to impose different obligations, we suggest use of consistent terms or wording.	
Likes 1	PPL - Louisville Gas and Electric Co., 6, Oelker Linn
Dislikes 0	
Thomas Rafferty - Edison International - Southern California Edison Company - 5	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	
Document Name	
Comment	

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP‑003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Tyson Archie - Platte River Power Authority - 5	
Answer	
Document Name	
Comment	

PRPA understands that the SDT is under time constraints in addressing Order No. 829, however, PRPA requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

PRPA requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

PRPA feels that all standards with requirements that apply to low impact assets should be included in CIP‑003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to PRPA if this was intentional for R3 and R4. PRPA requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Nick Braden, N/A, Braden Nick
Dislikes 0	

Steven Mavis - Edison International - Southern California Edison Company - 1	
Answer	
Document Name	
Comment	
Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison.	
Likes 0	
Dislikes 0	
Andrew Gallo - Austin Energy - 6	
Answer	
Document Name	
Comment	

AE understands that the SDT is under time constraints in addressing Order No. 829, however, AE requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

AE requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

AE feels that all standards with requirements that apply to low impact assets should be included in CIP-003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states “suppliers, vendors and other entities”. The Requirement language only references vendors. The SDT should clarify who or what “suppliers” and “other entities” are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard. Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to AE if this was intentional for R3 and R4. AE requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.	
Likes 1	Austin Energy, 4, Garvey Tina
Dislikes 0	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	
Comment	
Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5. This standard should be written using the Applicability Tables used in CIP-003 through CIP-011. As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard. Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource	

commitments including modifications to existing contracts and agreements to deliver desired solutions. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

Moify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

Move CIP-013 R2 into CIP-003-x R1 with other CIP policies that are reviewed by the CIP Senior Manager. This would also provide alignment across high, medium, and low impact Cyber Assets.

CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Janis Weddle - Public Utility District No. 1 of Chelan County - 6
Answer
Document Name
Comment

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.	
Likes 0	
Dislikes 0	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	
Document Name	
Comment	

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP-003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.	
Likes 0	
Dislikes 0	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	
I support the comments of Andrew Gallo at Austin Energy.	
Likes 0	
Dislikes 0	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	
Document Name	
Comment	

As written, implementation of this draft standard may degrade rather than improve reliability by interfering with the ability to respond and recover from BES cybersecurity events. The draft standard also encourages the use of a monoculture of products allowing broader damage from a single zero-day vulnerability.	
Likes 0	
Dislikes 0	
Joe McClung - Joe McClung On Behalf of: Ted Hobson, JEA, 5, 1, 3; - Joe McClung, Group Name JEA Voters	
Answer	
Document Name	
Comment	
We agree with the LPPC/APPA comments.	
Likes 0	
Dislikes 0	
Alan Farmer - ACEC/Burns & McDonnell - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

The American Council of Engineering Companies (ACEC) -the business association of the nation's engineering industry - wants to convey the industry's perspectives and concerns over the development of this new cyber security supply chain rule mandated by the Federal Energy Regulatory Commission (FERC).

ACEC member firms, numbering more than 5,000 firms representing over 500,000 employees throughout the country, are engaged in a wide range of engineering works that propel the nation's economy, and enhance and safeguard America's quality of life. Council members are actively involved in every aspect of the energy marketplace.

Supply chain cyber security is of growing concern to all our members. While we believe that present cyber security controls and voluntary practices are highly effective, input by engineering service providers would assist NERC/FERC in producing a more effective approach in minimizing the impacts on competition, risk allocation, and pricing.

In short, ACEC is in agreement with most of the comments of the owners, operators, vendors and suppliers that have formally participated in this Standard development. We fully appreciate the concerns over how risk can be adequately managed under any proposed standard. Our member firms' reputations depend upon professional performance and innovation in an atmosphere of collaboration. However, we are concerned that the supply chain language in this Standard will not support, and may actually impair, broad-based cost-effective infrastructure security and grid reliability

Likes 0	
Dislikes 0	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	
Document Name	
Comment	

CHPD understands that the SDT is under time constraints in addressing Order No. 829, however, CHPD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

CHPD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

CHPD feels that all standards with requirements that apply to low impact assets should be included in CIP-003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CHPD if this was intentional for R3 and R4. CHPD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Lona Hulfachor - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

SRP understands that the SDT is under time constraints in addressing Order No. 829, however, SRP requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

SRP requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

SRP feels that all standards with requirements that apply to low impact assets should be included in CIP‑003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to SRP if this was intentional for R3 and R4. SRP requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 1	Snohomish County PUD No. 1, 6, Lu Franklin
Dislikes 0	

Kenya Streeter - Edison International - Southern California Edison Company - 6
Answer
Document Name
Comment

Please refer to comments submitted by Deborah VanDeventer on behalf of Southern California Edison	
Likes 0	
Dislikes 0	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	
Document Name	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 4	
Answer	
Document Name	
Comment	
FirstEnergy recommends that the SDT take additional time in preparing a draft supply chain Standard that properly separates “supply chain” Requirements from additional operational and maintenance Requirements. Operational and maintenance Requirements should be added to	

the existing CIP Standards where the subject protections are already addressed. In addition, any Requirements applicable to Low Impact BES Cyber Systems should be placed in CIP-003 as has been established as a practice for all other low impact requirements. It should also be noted that certain expectations of these Requirements have economic implications to entities of all sizes. These Requirements could result in limiting the flexibility of an entity to obtain cyber assets from third-party distributors at a significant discount. For some entities, the additional costs could have an impact on their ability to remain for example, an economically viable generating unit. While probably not something that by itself impact the continued operation of a generating unit, the additional costs associated could be an influencing factor in keeping BES generating unit in-service.	
Likes 0	
Dislikes 0	
Aubrey Short - FirstEnergy - FirstEnergy Corporation - 1	
Answer	
Document Name	
Comment	
Support FirstEnergy Comments submitted by Aaron Ghodooshim – Segment 4).	
Likes 0	
Dislikes 0	
Mike Kraft - Basin Electric Power Cooperative - 5	
Answer	

Document Name	
Comment	
Basin Electric has concerns with being held accountable for vendors who not meet the attributes of this proposed Standard. Basin Electric prefers existing CIP standards be modified to satisfy the order. With the current FERC Commission lacking quorum, the timeframe to add commission members and the resulting backlog from the delay, it would appear the FERC Commission is not in a position to act upon a hastily constructed new standard. Basin Electric suggests NERC request an extension of time to modify existing standards to meet the order. Basin Electric suggests CIP-013 follow the table structure used in the existing enforceable CIP standards including the Part, Applicable Systems, Requirements and Measures.	
Likes 0	
Dislikes 0	
Kelly Silver - Con Ed - Consolidated Edison Co. of New York - 1, Group Name Con Edison	
Answer	
Document Name	
Comment	
Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5. This standard should be written using the Applicability Tables used in CIP-003 through CIP-011. Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource	

commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES. Recommend the following: Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance. Move CIP-013 R3, to CIP-010 R1. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 Move CIP-013 R5 to CIP-003 R2 Question – what about contracts negotiated during the implementation period? Are these contracts subject to this Standard? What about existing contracts? What about contracts that are renewed (evergreen contracts)? What about contracts initiated during the 15 calendar month review?	
Likes 0	
Dislikes 0	
Michael Ward - Seminole Electric Cooperative, Inc. - 4	
Answer	
Document Name	
Comment	
Seminole Electric comments submitted by Michael Haff	
Likes 0	

Dislikes 0	
William Harris - Foundation for Resilient Societies - 8	
Answer	
Document Name	Resilient Societies CIP 013-1 Comments 03042017.docx
Comment	
See comments in the attached file.	
Likes 0	
Dislikes 0	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	
Document Name	
Comment	
PJM agrees with the comments submitted by the SWG. Additionally, PJM suggests that 1.2.1 be stricken since it is ambiguous and already covered by 1.2.3 and 1.2.4. It is not clear what would be defined as a “vendor security event” that is outside of the events listed in 1.2.3 and 1.2.4.	
Likes 0	
Dislikes 0	

Rob Collins - Rob Collins On Behalf of: Scotty Brown, Southern Indiana Gas and Electric Co., 1, 6, 5, 3; - Rob Collins	
Answer	
Document Name	
Comment	

"This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement." - Verbiage to this effect needs to be part of the standard.

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	
Fred Frederick - Southern Indiana Gas and Electric Co. - 3	
Answer	
Document Name	
Comment	

Verbiage similar to the follwoing needs to be part of the standard. “This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.”

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Darnez Gresham - Darnez Gresham On Behalf of: Dehn Stevens, Berkshire Hathaway Energy - MidAmerican Energy Co., 1, 3; - Darnez Gresham

Answer	
Document Name	

Comment

Summary of comments direction:

1. No “plans.” (Delete R1 and R2). Order 829’s four objectives did not include creating “plans.”

2. All four of the directives either direct or use examples of specific operational cyber security controls which are best addressed as revisions to CIP-002 through -011. (Delete R3-5).

3. We recommend the CIP-013 SDT request NERC to assign the CIP revisions SDT to assist the CIP-013 team to draft the technical revisions for each of the four directives in CIP-002 through CIP-013. The CIP revisions SDT has met their Order 822 directive that had a deadline. To get the best standards for reliability and meet the FERC Order 829 directives' deadlines, NERC and industry should reprioritize SDT teams' work and resources. Result: No CIP-013 standard. Revised CIP-002 through -011 standards. Other comments: On the one hand Order 829 states intent to respect FPA section 215 jurisdiction by only addressing the obligations of responsible entities. A Reliability Standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to responsible entities. Yet, in paragraph 59, Order 829 states, "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." Contracts are bi-lateral and as such impose obligations on both parties, in direct contradiction to not imposing obligations on suppliers, vendors or other entities. Paragraph 59 is indirectly imposing obligations on suppliers, vendors or other entities that provide products or services to responsible entities. If the entity chooses, contracts can be a tool in "how" they deliver the "what" for the security objective. However, the registered entity's compliance has to be measured on achieving the security objective, not on contract terms. We will not support any standard that prescribes contract terms and makes contract terms a measure of an entity's compliance. Entities have been achieving the CIP-004 security objectives for background checks, training and access revocations since CIP version 1 without the prescription of "how" it had to be done (without making contract terms a measure of their compliance). We strongly agree with the Midwest Reliability Organization comments.	
Likes 2	Berkshire Hathaway Energy - MidAmerican Energy Co., 1, Harbour Terry; Jeffrey Watkins, N/A, Watkins Jeffrey

Dislikes 0	

Steve Rawlinson - Southern Indiana Gas and Electric Co. - 1

Answer	
Document Name	

Comment

"This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement." - Verbiage to this effect needs to be part of the standard.

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event.

Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply.

Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.

Likes 0	
Dislikes 0	

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6

Answer	
Document Name	

Comment
• During the Assess/Plan, Procure/Acquire phases of the Supply Chain process, separate requirements for standalone Standard (CIP-013) should be developed. For the deployment and operational aspects of the Supply Chain, appropriate requirements should be incorporated into the existing CIP Standards. It is recommended that this SDT collaborate with the CIP-002-CIP-011 SDT for language that can be used until R3 – R5 can be moved to their appropriate operational standards. • All measures sections will need to be updated to reflect any changes that are made to the requirements. • Dominion recommends that “remote access” should be changed to “electronic remote access” throughout the proposed CIP-013-1.

Likes 0	
Dislikes 0	

RoLynda Shumpert - SCANA - South Carolina Electric and Gas Co. - 1,3,5,6 - SERC

Answer	
Document Name	

Comment
The need to have supply chain risk management is agreeable; however, in its current form, CIP-013-1 poses a great challenge and burden to SCE&G and other Responsible Entities for various reasons, many of them documented in the Unofficial Comment Form. SCE&G recommends that CIP-013-1 include a modified R1 and R2 only, and not include R3 through R5. Requirements R1 and R2 focus on the supply chain and will suffice as an initial implementation step of supply chain risk management. The remaining requirements are operational obligations that need to be integrated into existing NERC CIP Standards.

Likes 0	
Dislikes 0	

David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	

Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standards.

Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Also recommend the following:

- Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.
- Move CIP-013 R3, to CIP-010 R1.
- CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6
- Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	
Alyssa Hubbard - SCANA - South Carolina Electric and Gas Co. - 5	
Answer	
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Brad Lisembee - Southern Indiana Gas and Electric Co. - 6	
Answer	
Document Name	
Comment	
Request verbiage similar to the following is added as part of the standard: This standard is forward looking in that it does not apply to current vendor relationships, systems, and processes, and does not require entities to renegotiate currently effective contracts in order to implement.	

Vectren would like definitions of security breaches, vendor-related cyber security incidents, security event, and vendor security event. Vectren respectfully requests FERC reconsider the timeline for this standard to allow additional time to identify the risks, and consequently, the appropriate controls. This would allow the SDT to outline the requirements so utilities are able to comply. Vectren is committed to the safety and reliability of the BES and committed to compliance excellence. We appreciate the efforts of the Standard Drafting Team and will be glad to provide any additional detail upon request. Thank you, again, for the opportunity for Vectren to provide comments on this draft standard.	
Likes 0	
Dislikes 0	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The California ISO supports the comments submitted by the ISO/RTO Council (IRC) and the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Quintin Lee - Eversource Energy - 1	
Answer	

Document Name	
Comment	
{C}1) Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5. {C}2) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011. {C}3) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references "suppliers, vendors and other entities". The Requirement language only references vendors. Provide guidance on who or what "suppliers" and "other entities" are, how they differ from vendors and how they are address in the CIP-013-1 standard. {C}4) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES. Recommend the following: {C}a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance. {C}b. Move CIP-013 R3, to CIP-010 R1. {C}c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 {C}d. Move CIP-013 R5 to CIP-003 R2	
Likes 0	
Dislikes 0	

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
In the Purpose, change “security controls” to “procurement and operational controls” as presented in the materials. CenterPoint Energy request that the SDT format CIP-013 like the other CIP Standards, a table design, if possible. CenterPoint Energy suggests more collaboration between the CIP Modifications SDT and the Supply Chain SDT to help eliminate overlap and better align with existing CIP requirements. In general, the SDT should consider the operational impacts that this standard could have on the industry. Flexibility is necessary.	
Likes 0	
Dislikes 0	
Nicolas Turcotte - Hydro-Qu?bec TransEnergie - 1	
Answer	
Document Name	
Comment	
HQT voted Negative and would like to see the following matters to be addressed:	

-CIP-013 should move forward with only R1 and R2 since they are mostly procurement related-some concern is being expressed that the requirements for having a supply chain risk management plan seem to a cover low medium and high BES Cyber assets as well as allowing entities to assess their own risk. Further clarification and perhaps some third party verification would be beneficial. -Contractual issues could exist. Although the FERC order doesn't require abrogation of contracts there is some concern that there could end up being multiple contracts in place, those newly negotiated and the existing ones. Confusion exists between use of terms vendor and suppliers in the draft standard and the Guidance section. -Concerns exist regarding authentication on multiple levels and how vendors and their manufacturers may combine hardware and software into their products and how there could meaningful verification and authentication -There are a number of areas where time seems to be an issue as it relates to implementation -Use of "applicability tables" as they appear in other CIP standards would clarify the requirements to alleviate compliance concerns - R3, R4 and R5 should move into existing CIP Standards to avoid P81 issues (redundancies) and ease implementation for Entities and improve auditability efficiencies.	
Likes 0	
Dislikes 0	
Ballard Mutters - Orlando Utilities Commission - 3	
Answer	
Document Name	
Comment	
OUC understands that the SDT is under time constraints in addressing Order No. 829, however, OUC requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of	

requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

OUC requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Likes 0	
Dislikes 0	

Lauren Price - American Transmission Company, LLC - 1

Answer	
Document Name	

Comment

In conclusion, ATC has concern that, despite what is a well-intended attempt by a highly qualified SDT to address the directives of FERC Order 829, CIP-013-1 is its current form is ultimately serving as an vehicle to revise or expand the scope and requirements to several currently approved and enforceable CIP Cyber Security Reliability Standards without affording the industry due process in accordance with the NERC Rules of Procedure for those modifications. 1.) Where existing Reliability Standards and Requirements meet the intent of CIP-013-1 and the FERC Order 829 directives, the existing Reliability Standards should be leveraged to accomplish the objective instead of creating a duplicative standard. 2.) Where Reliability Standards and Requirements may not go far enough to meet a given objective as it relates to vendors or suppliers, consideration should be given to modifying those existing Reliability Standards and Requirements, or perhaps investing time toward the further exploration of leveraging available standardized industry frameworks or practices that meet the objectives in an ever changing threat landscape as opposed to a reliability standard that a.) may be ill-equipped to keep pace with emerging threats and b.) perhaps carry the risk of hindering a Registered Entity's ability to be timely and nimble in addressing those threats in order to maintain compliance with a requirement(s) that has been rendered irrelevant. The creation of a new Reliability Standard should not supersede, contradict, expand,

amend, or otherwise effectively revise other currently approved and enforceable CIP Cyber Security Reliability Standards. Those Standards exposed to this condition are cited in other comments and include, at a minimum the below listed five (5) CIP Standards:

- CIP-002-5.1
- CIP-003-6
- CIP-004-6
- CIP-005-5
- CIP-007-6

In conclusion, the above concerns related to redundancy or contradiction to approved and enforceable CIP Standards, the cited expansion to the FERC directives, and the confusion, inconsistency, and broad sweeping language that is at odds with the intent of both enforceable CIP Standards, the effort of paragraph 81, and FERC Order 829 supports the wisdom and caution within FERC Commissioner's (Cheryl A. LaFleur's) dissent to FERC Order 829. LaFleur's dissent to FERC Order 829. (P. 67) issued on July 21, 2016, cautions that "**…effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, technical, economic, and business relationship issues**." In this dissent, LaFleur acknowledges that the threat of inadequate supply chain risk management procedures poses a very real threat to grid reliability; and while LaFleur offers full support of the Commission's continued attention to this threat, LaFleur's **"…fear that the flexibility** *[within FERC Order 829]* **is in fact a lack of guidance and will therefore be a double-edged sword.**" is demonstrable in this first draft of CIP-013, and further evidence that FERC Order 829 may have been premature thereby causing a highly qualified and well-intended SDT to be ill-equipped to "**…translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act.**" With Cheryl A. LaFleur's recent appointment to FERC's Acting Chairman on January 23, 2017, ATC respectfully encourages NERC and the SDT to consider if there is an opportunity for FERC to revisit the need for the CIP-013-1 Supply Chain Reliability Standard and to reevaluate the appropriateness and viability of FERC Order 829 and whether or not the SDT should move forward or if FERC Order 829 should be rescinded in favor of the industry leveraging the existing CIP-002 – CIP-011 approved and enforceable reliability standards in combination with the risk-based industry standards and frameworks as an alternative approach to drafting this new Reliability Standard. ATC thanks the SDT for consideration of our positions.

Likes 0	

Dislikes 0	
Warren Cross - ACES Power Marketing - 1,3,4,5 - MRO,WECC,Texas RE,SERC,SPP RE	
Answer	
Document Name	
Comment	

1. We believe in finding a beneficial multi-sector solution that will lower costs, encourage innovation, and support among multisector vendors.

2. The current standard would create a compliance burden for entities that are already resource constrained.

3. We believe that the SDT should focus on a supply chain management standard that is designed to:

· Manage in addition to eliminating risk;

· Ensure that operations are adapting to constantly evolving threats;

· Be aware of and responsive to changes within their own organization, programs, and the supporting information systems; and

· Adjust to the rapidly evolving practices of the electricity sector's supply chain.

4. Though the current language would certainly raise standards across the entirety of the software industry, it could result in isolation of the electricity sector and hamper growth and innovation among industrial control vendors.

5. We thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	
Document Name	
Comment	
Reclamation commends the SDT for the draft that was provided for a new and complex standard in a short amount of time. Reclamation recommends a more simplified format of the proposed standard. Reclamation believes that the objectives and intent and of FERC Order 829 can be met without spelling out each objective as a separate requirement. As presently written, the first draft contains repeating elements (such as access, authentication, product delivery, etc.) in different requirements. The simplified approach described in the answers to Questions 1 through 5 above would eliminate redundancy.	
Likes 0	
Dislikes 0	
Shawn Abrams - Santee Cooper - 1, Group Name Santee Cooper	
Answer	
Document Name	
Comment	
Santee Cooper understands that the SDT is under time constraints in addressing Order No. 829, however, the SDT should carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of	

requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Santee Cooper requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

Santee Cooper recommends that all standards with requirements that apply to low impact assets be included in CIP‑003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear if this was intentional for R3 and R4. Santee Cooper requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Santee Cooper recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, Santee Cooper agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and Santee Cooper urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address gaps remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns that does not advance the security of the grid, as set out by now-Chairperson LaFleur in her dissent to Order 829.

Likes 0	
Dislikes 0	

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
FERC Order no 829 (p21) discusses “suppliers, vendors and other entities”. CIP-013-1 only refers to vendors. BPA suggests that the SDT clarify the scope and define any appropriate differences applicable to supplier, vendors or other entities.	
Likes 0	
Dislikes 0	
Nathan Mitchell - American Public Power Association - 3,4	
Answer	

Document Name	
Comment	

1) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

2) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references "suppliers, vendors and other entities". The Requirement language only references vendors. Provide guidance on who or what "suppliers" and "other entities" are, how they differ from vendors and how they are address in the CIP-013-1 standard.

3) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource commitments including modifications to existing contracts and agreements to deliver desired solutions. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES.

Recommend the following:

a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance.

b. Move CIP-013 R2 into CIP-003-x R1 with other CIP policies that are reviewed by the CIP Senior Manager. This would also provide alignment across high, medium, and low impact Cyber Assets.

c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6

d. Move CIP-013 R5 to CIP-003 R2

Likes 0	
Dislikes 0	

Glenn Pressler - CPS Energy - 1

Answer	
Document Name	
Comment	
CPS Energy supports the comments provided by ERCOT and APPA	
Likes 0	
Dislikes 0	
Sheranee Nedd - Public Service Enterprise Group, Public Service Electric & Gas, PSEG Fossil LLC, PSEG Energy Resources & Trade LLC - 1,3,5,6 - NPCC,RF, Group Name PSEG REs	
Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Shannon Fair - Colorado Springs Utilities - 6, Group Name Colorado Springs Utilities	
Answer	
Document Name	

Comment
Colorado Springs Utilities (CSU) understands that the SDT is under time constraints in addressing Order No. 829, however, CSU requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1. CSU requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3. CSU feels that all standards with requirements that apply to low impact assets should be included in CIP‑003. As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard. Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to CSU if this was intentional for R3 and R4. CSU requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each. CSU requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.

Likes 0	
Dislikes 0	

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Document Name	
Comment	

While there are different ways to approach the complex issues of the supply chain risk, a proactive approach to address the issue can only help improve the industry's security posture. The difficulty in addressing the complexities requires additional evaluation to address the issues impacting both the development and implementation of solutions. Similar to CIP-014, the development of Supply Chain Risk Management plans and procurement process proposed under R1 and R2 may be appropriate within a new or revised Reliability Standard. The technical controls proposed for CIP-013 R3 and R4 may be better addressed within existing CIP Standards. The IESO abstains from commenting on R5 but believes integration into existing CIP Standards might be appropriate, especially since CIP-003 Attachment 1 already is comprised of a security plan.

This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. This is applicable to Requirements 1, 3, 4, and 5. The plan should allow for risk acceptance and leverage of an exception process. To address these concern, the drafting team should include some provisional or exception language to protect Responsible Entities such as use of a Technical Feasibility Exception (TFE). NERC's Appendix 4D to the Rules of Procedure provide for a basis of approval of a TFE beyond strict technical limitations of a system. Reference Section 3.0 of the appendix for more information.

The Standard uses "supplier" and "vendor" throughout, interchangeably. The terms should be consistent throughout to avoid confusion.

Likes 0	
Dislikes 0	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	

Document Name	CIP-013 Comment Mar 2 revision SCL 2017-3-6.docx

Comment

The attached document has comments compiled for all the questions. Please note that the BOLD paragraphs below (YELLOW highlighted in attachment) are uniquely Seattle City Lights. The un-highlighted comments were developed in collaboration with other entities and trade organizations such as LPPC. These comments may be like those submitted by other entities but not necessarily. City Light recognizes the challenges facing the SDT and appreciates the efforts the SDT is placing into working towards developing a solid standard.

Seattle City Light understands that the SDT is under time constraints in addressing Order No. 829, however, Seattle City Light requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.

Seattle City Light requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively, this could be addressed as an Exemption in Section 4.2.3.

Seattle City Light feels that all standards with requirements that apply to low impact assets should be included in CIP-003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to Seattle City Light if this was intentional for R3 and R4. Seattle City Light requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

As discussed in comments to R1 above, Seattle City Light requests that the title of the standard be changed to "Vendor Risk Management" to clarify that the scope of the required activities relate to the relationships among a utility and its vendors. In common usage, the term "supply chain risk management" encompasses a much broader scope of concerns, including quality control and verification of third-party

suppliers as well as addressing sole-source and international dependencies. Although the FERC Order and SDT white paper cite concerns about both vendor risk and supply chain risk, the requirements actually proposed in CIP-013 address vendor risk.

Seattle City Light recognizes the importance of regulatory bodies and the regulatory industry jointly addressing issues concerning cybersecurity and the reliability of the bulk electric system. In this standard, City Light agrees with other industry comments that many of the gaps addressed in CIP-013 should be modified in other standards and not established as a new standard nearly duplicative of (or worse, in conflict with) other standards. FERC provided NERC the opportunity to either develop a new or modified standard, and City Light urges the SDT to pursue the latter option as much as is appropriate. Requirements in CIP-013 to address the gaps that remain must be carefully crafted to avoid creating an ineffective, unauditable and unenforceable standard. Additionally, the short timeframe for submission of this standard and implementation period restricts the utility industry from contributing meaningful and thoughtful comments that would better focus on supply chain concerns. Thus this standard "does not advance the security of the grid," as set out by now-Chairperson LaFleur in her dissent to Order 829.

Likes 0	
Dislikes 0	

Chris Gowder - Chris Gowder On Behalf of: Carol Chinn, Florida Municipal Power Agency, 5, 6, 4, 3; Chris Adkins, City of Leesburg, 3; David Schumann, Florida Municipal Power Agency, 5, 6, 4, 3; Don Cuevas, Beaches Energy Services, 1, 3; Ginny Beigel, City of Vero Beach, 3; Joe McKinney, Florida Municipal Power Agency, 5, 6, 4, 3; Ken Simmons, Gainesville Regional Utilities, 1, 3, 5; Lynne Mila, City of Clewiston, 4; Richard Montgomery, Florida Municipal Power Agency, 5, 6, 4, 3; Tom Reedy, Florida Municipal Power Pool, 6; - Chris Gowder, Group Name FMPA

Answer	
Document Name	

Comment

FMPA agrees with comments submitted by American Public Power Association.

Likes 0	
Dislikes 0	
Payam Farahbakhsh - Hydro One Networks, Inc. - 1	
Answer	
Document Name	Hydro One_Unofficial_Comment_Form_CIP-013-1-First Draft.docx
Comment	

We suggest that the standard should have two requirements only.

R1 could require the entities to identify risks, evaluate controls (at minimum the controls itemized in FERC Order), and implement controls based on the acceptable level of risk to address the four objectives in FERC Order and mitigate risks stated in the Order.

R2 could be the periodic review and approval of R1 by CIP Senior Manager.

The applicability could be to all BES Cyber Systems essential for operation of BES. Entities should consider impact rating of High, Medium and Lows when evaluating necessary controls.

Comment for consideration in the RSAW

For the RSAW and under Requirement 1 in the section called “Note to the Auditor”, We recommend adding that “Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan” as stipulated in the Rationale for Requirement 1.

Likes 0	
Dislikes 0	

Erick Barrios - New York Power Authority - 5	
Answer	
Document Name	
Comment	
The NYPA Comments	
Likes 0	
Dislikes 0	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	
Document Name	
Comment	
SMUD understands that the SDT is under time constraints in addressing Order No. 829, however, SMUD requests that the SDT carefully evaluate each element of the proposed requirements against closely related existing CIP requirements to ensure there is no overlap or duplication of requirements. For example, removal of vendor remote or onsite access (CIP-013, R1.2.2) is perhaps sufficiently if not identically addressed in CIP-004 R5, P5.1 and interactive remote access (CIP-013, R1.2.6) is addressed in CIP-005 R2, P2.1.	

SMUD requests adding language comparable to a CIP Exceptional Circumstance for each of the requirements to address circumstances where compliance cannot be achieved due to a vendor's inability to conform to any requirements or an entities policies or plans. Alternatively this could be addressed as an Exemption in Section 4.2.3.

SMUD feels that all standards with requirements that apply to low impact assets should be included in CIP-003.

As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states "suppliers, vendors and other entities". The Requirement language only references vendors. The SDT should clarify who or what "suppliers" and "other entities" are, how, if at all, they differ from vendors, and how they are addressed in the CIP-013-1 standard.

Requirement R1 applies to BCS and associated EACMS, PACS, and PCA. The other requirements only apply to BCS. This makes sense for R5 since it only applies to low impact systems and EACMS, PACS, and PCA are not low impact terms. However, it is unclear to SMUD if this was intentional for R3 and R4. SMUD requests that the SDT look at the scope of each requirement and verify the intended systems are identified in the language of each.

Likes 0	
Dislikes 0	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI members prefer use of the applicability tables, especially for R3 and R4.

EEI commends the work done by the SDT and NERC on this difficult task. CIP-013 is a challenging standard given it is focused on minimizing risk introduced by third parties that the Responsible Entities have little control over. In particular, we are reminded of Acting Chairman LaFleur's

dissenting statement “effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, economic, and business relationship issues.” In addressing our comments and others, we recommend that the SDT focus on the security objectives and what the Responsible Entities can do in procurement to minimize risk to the bulk-power system. Although cybersecurity is a risk, other risks such as reliability may outweigh the need for certain cybersecurity focused requirements. Cybersecurity is about managing risk, which must be balanced against a number of factors and for the electricity subsector, keeping the lights on is key.	
Likes 0	
Dislikes 0	
Marc Donaldson - Tacoma Public Utilities (Tacoma, WA) - 3	
Answer	
Document Name	
Comment	
Tacoma concurs with the comments provided by the LPPC.	
Likes 0	
Dislikes 0	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	

Answer	
Document Name	
Comment	
BANC supports the comments filed by Sacramento Municipal Utility District	
Likes 0	
Dislikes 0	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Document Name	
Comment	
While there are different ways to approach the complex issues of the supply chain risk, a proactive approach to address the issue can only help improve the industry's security posture. The difficulty in addressing the complexities requires additional evaluation to address the issues impacting both the development and implementation of solutions. Similar to CIP-014, the development of Supply Chain Risk Management plans and procurement process proposed under R1 and R2 may appropriate within a new or revised Reliability Standard. The technical controls proposed for CIP-013 R3 and R4 may be better addressed within existing CIP Standards. The IRC abstains from commenting on R5 but believes integration into existing CIP Standards might be appropriate, especially since CIP-003 Attachment 1 already is comprised of a security plan. This requirement puts a substantial responsibility on the Responsible Entity without any authority or recourse if the vendor is unwilling or unable to agree. This is applicable to Requirements 1, 3, 4, and 5. The plan should allow for risk acceptance and leverage of an exception process. To address these concern, the drafting team should include some provisional or exception language to protect Responsible Entities	

such as use of a Technical Feasibility Exception (TFE). NERC's Appendix 4D to the Rules of Procedure provide for a basis of approval of a TFE beyond strict technical limitations of a system. Reference Section 3.0 of the appendix for more information. The Standard uses "supplier" and "vendor" throughout, interchangeably. The terms should be consistent throughout to avoid confusion	
Likes 0	
Dislikes 0	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	
Document Name	
Comment	
We appreciate the significant efforts of the SDT to develop this draft standard on difficult subject matter in such a short amount of time. However, based upon this initial draft, it is evident that additional time is necessary for the SDT to develop an effective standard addressing supply chain security risks. We suggest that the SDT develop a formal recommendation to NERC staff requesting that NERC file for an extension of time to collect additional stakeholder feedback in order to develop a more effective standard. In general, we request that the SDT consider our comments in question 1 that supply the following framework for a supply chain security standard: FERC's directives in paragraphs 43 through paragraph 62 summarized a general framework for this new Standard as outlined: R1: Develop a plan to include security controls for supply chain management that include the following four specific security objectives in the context of addressing supply chain management risks: R1.1 Security objective 3 (*information system planning*)	

R1.2 Security objective 4 (*vendor risk management and procurement controls*)

R1.3 Security objective 1 (*software integrity and authenticity*)

R1.4 Security objective 2 (*vendor remote access*)

R2: Implement the plan specified in R1 in a forward looking manner.

R3: Review and update, as necessary its supply chain cyber security risk management plan(s) specified in R1 at least once every 15 calendar months

R3.1 Evaluation of revisions…

R3.2 Obtaining CIP Senior Manager or delegate approval.

GTC feels this framework outlined above satisfies Order 829 in the context of addressing supply chain management risks, completely. Although FERC expressed some operational scenarios of existing CIP standards not explicitly addressing supply chain risks, the point of FERC's summary was still in the context of addressing supply chain risks and not additional operational controls as presented by the SDT.

From a clarity standpoint, we urge the drafting team to consider limiting the structure of CIP-013-1 to the supply chain horizon which ends at the delivery of products/services to the acquirer in accordance with NIST SP 800-53 r4 rather than a holistic BES Cyber System Life Cycle approach chosen. GTC submits that the operations and maintenance of BES Cyber systems are already addressed in existing standards. Lastly, FERC provides NERC discretion per paragraph 44 the option of modifying existing Reliability Standards to satisfy the directive, so if the SDT believes additional operational gaps still exist, then GTC prefers NERC identify these risks, and explain to FERC NERC's intent to invoke operational changes by modifying existing CIP requirements with the submission of a "supply chain horizon contained" CIP-013-1.

Lastly, GTC recommends the SDT develop a Guidelines and Technical Basis section to be included within the standard for clarifications of the following…" ***Who is the vendor? Is it the manufacturer/software company, the reseller the hardware/software is acquired from, the shipping company, the integrator, others? For temporary staff, is the contract employee a vendor?***"

Likes 0	
Dislikes 0	

Bob Case - Black Hills Corporation - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
The intent of FERC Order 829 is noble, but seems to be directed to the wrong audience. The risks of compromised hardware and software impacts much more than ICS, in that it extends to all our processing and communication systems. With the advancement of IoT, the spirit of FERC Order 829 needs to be moved to an even higher national focus. In the meantime, NERC should focus on helping registered entities improve its controls culture within the activity environment it can directly impact. Thanks.	
Likes 0	
Dislikes 0	
Devin Elverdi - Colorado Springs Utilities - 1	
Answer	
Document Name	
Comment	
Refer to CSU comments.	
Likes 0	
Dislikes 0	

Maryanne Darling-Reich - Maryanne Darling-Reich On Behalf of: Eric Egge, Black Hills Corporation, 1, 3, 6, 5; - Maryanne Darling-Reich	
Answer	
Document Name	
Comment	
See comments submitted by Black Hills Corporation	
Likes 0	
Dislikes 0	
Bob Reynolds - Southwest Power Pool Regional Entity - 10	
Answer	
Document Name	
Comment	
By not modifying the existing CIP Standards where there is overlap of requirement, there is a distinct possibility of inconsistent policies and procedures. Furthermore, should the Registered Entity choose to reference its other Standards compliance documents, there is a possibility of creating circular references or “spaghetti” linkages.	
Likes 0	
Dislikes 0	

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	
Document Name	
Comment	
Avista commends the SDT and NERC for the extensive work done on developing this standard. Avista also supports the comments filed by the Edison Electric Institute (EEI).	
Likes 0	
Dislikes 0	

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion and NextEra	
Answer	
Document Name	
Comment	

1) Suggest that CIP-013 R1 and R2 are managerial controls and should be the only CIP-013 Requirements. The technical controls in R3 – R4 – R5 should be added to existing CIP Standards. For details, see comments on R3, R4 and R5.

2) This standard should be written using the Applicability Tables used in CIP-003 through CIP-011.

3) As quoted in the Guideline and Examples document, FERC Order no 829 (p21) states references “suppliers, vendors and other entities”. The Requirement language only references vendors. Provide guidance on who or what “suppliers” and “other entities” are, how they differ from vendors and how they are address in the CIP-013-1 standard.

4) Several the CIP-013 requirements are included in existing CIP standards or align more closely with the existing CIP standards that require process(es) or programs. The implementation for the current CIP-013 standard is short, 1 year, yet will required significant resource

commitments. Implementation per Entity Asset and Cyber Asset based upon procured services will be burdensome paperwork exercise to Entities creating focus upon compliance paperwork verses the desired results of improved security for the BES. Recommend the following: a. Modify CIP-013 to define the Cybersecurity Supply Chain program focused on managerial controls for procurement and maintenance. b. Move CIP-013 R3, to CIP-010 R1. c. CIP-013 R4 modify CIP-005 R2 , CIP-007 R4 Subpart 4.1.5 and/or CIP-008 R1 part 1.6 d. Move CIP-013 R5 to CIP-003 R2	
Likes 0	
Dislikes 0	
Philip Huff - Arkansas Electric Cooperative Corporation - 3,4,5,6	
Answer	
Document Name	
Comment	
This Standard implies a high degree of compliance audit and enforcement authority for the Regions, which we have not seen implemented. From our experience with CIPv5 compliance exceptions, the objectives of the Reliability Assurance Initiative to provide risk-based process efficiencies have not been met. Entities must still use the costly self-report process for anything short of perfection, and regional auditors are not given latitude to make risk-based decisions. CIP-013-1 as drafted cannot work as intended until entities can work with regional auditors to quickly assess risk.	
Likes 0	

Dislikes 0	
George Tatar - Black Hills Corporation - 5	
Answer	
Document Name	
Comment	
See Black Hills Corp comments	
Likes 0	
Dislikes 0	
Wes Wingen - Black Hills Corporation - 1	
Answer	
Document Name	
Comment	
The intent of FERC Order 829 is good, but seems to be directed to the wrong audience. The risks of compromised hardware and software impacts much more than ICS, but extends to all our processing and communication systems. With the advancement of IoT, the spirit of FERC Order 829 needs to be moved to an even higher national focus. In the meantime, NERC should focus on helping registered entities improve its controls culture within the activity environment it can directly impact. Thanks.	
Likes 0	
Dislikes 0	

Jamie Monette - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
We generally agree with EEI's comments, except for the exclusion of EACMS, PACs and PCAs for Requirement 1.	
Likes 0	
Dislikes 0	
Douglas Webb - Douglas Webb On Behalf of: Chris Bridges, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Harold Wyble, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; James McBee, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; Jessica Tucker, Great Plains Energy - Kansas City Power and Light Co., 3, 6, 5, 1; - Douglas Webb	
Answer	
Document Name	
Comment	
Note of Appreciation We recognize the constraints imposed on the Standard drafting process by the language of the Commission's Order and its directives. We also would highlight Commissioner LaFleur's caution--that the Order was premature—may be coming to fruition. In consideration of both points, we are appreciative of the Standard Drafting Team's continuing work on the CIP Cyber Supply Chain Standard and its efforts to overcome the challenges it presents. Thank you. Kansas City Power and Light Company	

Likes 0	
Dislikes 0	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	
Document Name	
Comment	
Oxy supports the comments of MRO.	
Likes 0	
Dislikes 0	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	
Document Name	
Comment	
The current version of CIP-013-1 is vague. Though flexibility is needed, the current version does not provide enough clarification to Registered Entities on the expectations required under the Standard and will therefore fail to mitigate cyber security risks to the BES.	
Likes 0	
Dislikes 0	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	
Document Name	
Comment	

We have several questions and concerns about what the phrases "vendor-initiated" and "system-to-system remote access" used in several requirements exactly mean. 1) Can the SDT please clarify what is meant by “vendor-initiated”. For example, if we (the customer) are having an operational issue and contact the vendor for support, is that support session still considered “vendor-initiated”, or would that session not be in scope because it is prompted by the customer’s request? Alternatively, if we initiate the remote access session with the vendor and turn over control to them, is that session still considered "vendor-initiated"? 2) We are unclear what the phrase "system-to-system" means. Please define or give examples of what would be considered a “system-to-system remote access with a vendor”. We are having trouble understanding how we might apply R4.1-4.3 and other associated requirements if there is no human interaction. 3) In our experience, vendor or third-party remote assistance is typically needed in times where there is a problem that could not be resolved by internal staff. We are concerned with the monitoring requirement (4.2), especially in situations where the system issue is having a real-time impact on operations and requires speedy trouble-shooting and resolution. There may not be enough internal resources available to respond to the situation and also actively monitor the vendor’s session. Additionally, the use of the phrase “unauthorized activity” is problematic, as the situation may not allow for a step-by-step explanation from the vendor as to what steps they are taking to troubleshoot the issue. Finally, how would one prove in an audit that the session was monitored and that no unauthorized activity occurred?

Tri-State strongly believes the directives issued in Order No. 829 should be addressed by revising existing CIP standards, so that entities have all the relevant requirements together. We are concerned that if the existing standards are not revised to incorporate the new requirements, we will recreate the confusion and complexity that came with v3 standards, which in many cases led to non-compliance. We encourage NERC to request more time from FERC to get this right the first time and to avoid future projects, if extra time is needed, and instead allow the industry to focus more time and resources on getting cyber security right.

Likes 0	

Dislikes 0	
Linsey Ray - Linsey Ray On Behalf of: Lee Maurer, Oncor Electric Delivery, 1; - Linsey Ray	
Answer	
Document Name	
Comment	
Concur with EEI's Position	
Likes 0	
Dislikes 0	
Val Ridad - Silicon Valley Power - 1 - WECC	
Answer	
Document Name	
Comment	
- See APPA's comments.	
Likes 0	
Dislikes 0	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA thanks the SDT for its work on this challenging project in such a short amount of time.	
Likes 0	
Dislikes 0	
Luis Rodriguez - El Paso Electric Company - 6	
Answer	
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.	
Likes 0	
Dislikes 0	

Pablo Onate - El Paso Electric Company - 1	
Answer	
Document Name	
Comment	

EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item.

EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.

Likes 0	
Dislikes 0	

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	

We appreciate the hard work of the standard drafting team in putting together this first draft standard and supporting documents. This is a very different type of standard than usual that asks entities to address risks that may be introduced by activities outside of their control. Although we have concerns with this first draft, we feel confident that the team can work through the issues and come up with a reasonable set of requirements.

If low impact Cyber Systems are included in any of the requirements, the requirements should be less stringent than those for high and medium since the risk to the BES is considerably less. Some of the other CIP standards use applicability tables to more clearly illustrate the

specific requirements for each of these impact levels (see CIP-004 for an example). If there are any variations in requirements for the impact levels – especially if low impacts are included in this standard - we would like to see the tables used. They provide consistency with the way the other standards are written, they're easier to navigate, and they can illustrate the risk-based nature of the standard.	
Likes 1	Public Utility District No. 2 of Grant County, Washington, 1, Sell Michiko
Dislikes 0	
Victor Garzon - El Paso Electric Company - 5	
Answer	
Document Name	
Comment	
EPE shares the comments and concerns voiced by the Edison Electric Institute (EEI) in this Ballot #1. Please refer to the EEI ballot for detailed comments on this item. EPE looks forward to working collaboratively with NERC staff and stakeholders in clarifying the wording of the various requirements to achieve more effective, efficient and widespread compliance on these important matters.	
Likes 0	
Dislikes 0	
Scott Kinney - Avista - Avista Corporation - 3	
Answer	
Document Name	

Comment	
Support EEI comments.	
Likes 0	
Dislikes 0	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
The drafting team should consider addressing some sort of vendor certification process to enable entities to select vendors that meet all of the security requirements stated within this standard. This will enable entities to rely on these vendors while allowing the entity to expeditiously address security vulnerabilities and other risks to operations.	
Likes 0	
Dislikes 0	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	

At the outset, Southern Company wishes to first note for the record its belief that Requirement R3 and Requirement R4 should be removed from the CIP-013 standard. As explained below, it is either duplicative of R1, duplicative of existing requirements in CIP-004-6, CIP-005-5, CIP-007-6, CIP-008-5, and CIP-010-2, and is inappropriate for a standard focused on the Supply Chain time horizon.

First, from the perspective of a supply chain procurement time horizon, verification of the integrity and authenticity of software and firmware is already addressed under Requirement R1, R1.2.3. Specifically, R1 requires a risk management plan that addresses controls for mitigating cybersecurity risks for industrial control system vendor products and services, and the plan must address methods to evaluate controls to address those risks (R 1.2) including "process(es) for verifying software integrity and authenticity of all software and patches that are intended for use". (R 1.2.3) Specifically, (assuming R1 covers only the procurement time horizon), then R3's requirement -- to implement "one or more documented processes" to address the verification of the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems -- is arguably covered by R1.2.3's requirement to have a process to do the same with respect to all industrial control system software and patches.

Second, to the extent R1 or R3 could be read to extend to verification of authenticity/integrity beyond the procurement and into the operational phase, such a broad interpretation should be outside of the scope of the CIP-013 supply chain standard, and would be more appropriately addressed in a separate proceeding to look specifically at operational standards CIP-002 through CIP-010. Specifically, patch monitoring and management is already described in CIP-007, yet little consideration appears to have been given to the burdensome impacts that might result on CIP-007 compliance if CIP-013 R3 compliance is layered on top in the operational time horizon, rather than being limited to the procurement phase (and thus covered in CIP-013 R1). The stringent 35 day cycles required within CIP-007-6 R2 will be significantly impacted by the proposed language in R3, placing Responsible Entities in a position of compromising compliance with one standard by trying to maintain compliance with another. The supply chain NOPR and final were not originally focused on these types of operational controls, and any such exploration of operational risk issues are more appropriately explored separately and outside of the supply chain proceeding. Moreover, if this standard is intended to cover all aspects of all lifecycle stages (from planning to procurement to production to retirement, i.e., cradle to grave) for all devices and vendors – that is an expansive initiative that overlaps with multiple CIP standards and would require a timeframe for development that is much longer than one year.

Similarly and for the above reasons, Requirement R4 is also considered not necessary and should be removed. The proposed requirement for "authorization of vendor remote access" is already explicitly required in CIP-004-6 R4; logging and monitoring of vendor remote access is already covered in CIP-005-5 R1 and CIP-007-6 R4; and response to "unauthorized activity" by vendors is already covered in CIP-008-5. The modifications provided above and suggested under R4 are to address the Responsible Entity having the capability to quickly disable vendor

remote access sessions, which again we strongly recommend the SDT consider incorporating into CIP-005 as a new requirement addressing this potential security improvement. Overall, industry was not given an adequate chance to express this in the FERC proceeding leading to Order 829 because the NOPR expressed proposed directives at a very broad and high level whereas the Final Rule contained much more prescriptive directives. Southern Company agrees with the July 21, 2016 statement provided by Acting Chairman LaFleur in this proceeding that "the more prudent course of action" for NERC, industry, and stakeholders would have been to issue a supplemental NOPR to provide input on the more prescriptive directives contained in this Final Rule. Southern Company would encourage an opportunity for input on such larger matters once the standard is submitted to the Commission for approval. Having said that, Southern Company recognizes and appreciates that, at this stage of standard development, NERC is bound to comply with the final rule's directives in Order 829. Therefore, while wishing to preserve for the record its opinion that Requirement R3 and R4 should be removed, Southern Company offers the comments and language contained herein to improve the standard from its currently drafted version.	
Likes 0	
Dislikes 0	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	
Document Name	
Comment	
ITC agrees with the comments submitted by EEI.	
Likes 0	
Dislikes 0	

Dennis Sismaet - Northern California Power Agency - 6	
Answer	
Document Name	
Comment	
I support the comments submitted by Brian Evans-Mongeon, Utility Services, Inc, and Marty Hostler, Northern California Power Agency.	
Likes 0	
Dislikes 0	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
Likes 0	
Dislikes 0	
Foundation for Resilient Societies Comments on Draft Standard 2016-03, Cyber Security Supply Chain Risk Management, NERC CIP 013-01	
1. Vote “NO” on approval of the draft.	

Rationale: The proposed CIP-013-01 standard is onerous and not cost-effective. It excpectss too much of individual registered entities, which should not be the primary organizations responsible for strengthening the integrity of the cyber supply chain.
Starting at the foundry level, it is essential to assure the integrity of chip design, manufacture and operations. And control of firmware by entities that are committed to protect the national security interests of the United States and Canada. The current practice of purchasing control and telecommunication systems from the lowest-cost supplier may be too risky and too imprudent to attain greater integrity in cyber supply chains. It is unreasonable to expect that some 1400 separate electric utilities should be responsible for major changes in the development and regulation of cyber supply chain systems.
The recent re;port on Cyber Deterrence by the Defense Science Board, released on February 28, 2017, seeks tailored initiatives to enhance deterrence of cyber attacks on critical infrastructures. This Report recognizes that a key element of deterrence is to improve defenses, so the payoffs to foreign adversaries will be reduced. Meanwhile, the Trump Administration has underway a review of cyber policies and strategy. If the Administration will support initiatives to strengthen cyber supply chains that involve indigenous U.S. design, production, operation, and integrity testing for the entire cyber supply chain, any final NERC-FERC standard responsive to Order No. 829 should await opportunities to be presented by the Administration after its policy review.
As a result of this overburden on registered entities, the Standard Drafting team -- not surprisingly -- has drafted CIP-013-1 containing too many exceptions, qualifications, and outstanding conflicts to form the foundation for the most-difficult process of managing the risks that derive from vulnerabilities in products marketed to the industry in a global and highly competitive environment. If some foreign governments subsidize their hardware systems, is it imprudent to always accept the lowest price products that place our cyber supply chains at risk?
The present draft standard makes the probability of successful discrimination exceedingly low. The investment of time and money by utilities and the industry will be very high, and certainly not worth the risks of failing compliance by entities and their procurement selections that are even further removed from technical competencies essential to their task.
Implementation as written will only encourage a shell game that will delay real solutions to the Supply Chain vulnerabilities and provide false assurances that must be addressed collectively by the industry, by state and by federal authorities. The latter must address the increasing failures of vendors to design secure products through market motivations and penalties. This problem has been successfully addressed in many other industries where serious safety issues existed.

2. Requirement R1

a. Any deep examination of the four objectives of R1 reveals substantial gulfs with the realities of Supply Chain issues.
   - Risks can never be assessed in the absence of vulnerability assessments. None are called for. And vulnerabilities range from individual components to full systems. End-to-end control center to remote unit network assessments are needed.

- A component flaw might trace to a vendor several stages removed from the utility and vulnerabilities are often the product of several vendors' missteps.
- Adversarial efforts impact multiple systems and subsystems; hardware and software and firmware, classical attack vectors and subtleties difficult for even professional forensic experts. These challenges are beyond utilities' ability to assess.
- The "prior contract" exclusion leaves open vulnerabilities introduced post "contracting." Note that the February 2017 Defense Science Board Report on Cyber Deterrence calls for improvements in defensive capabilities as a key element of deterrence. The "prior contract" exception will assure access by foreign adversaries that will enable continuing implantation of malware, continuing exercise of equipment within the U.S. electric grid and within other critical infrastructures upon which the North American electgric grid depends. . These"prior contract" exceptions are inexcusable; a program needs to be developed -- not by individual registered entities -- to assist in the removal and replacement of hazardous hardware, firmware, and software.
- The absence of hard requirements for "secure vendor accesses", "Internet avoidance", "encryption", "blacklisting known malware", etc. reveals industry ambivalence re: enforceable supply chain controls.
- No plan can possibly be developed that will adequately cover the variety of situations and conditions that exist. They are far too complex to be "planned for" separately by over 1400 independent "Responsible Entities". And we observe the usual escape clause, ***"Obtaining specific controls in the negotiated contract may not be feasible and it is not considered failure to implement an entity's plan".*** How does one define ***success***, under these circumstances?

b. **Requirement R2**. The R2 process is clearly a bureaucratic device; an artificial deadline for updating the plan, get approval from the senior CIP manager (who should have sustained involvement, not at 15 month intervals.) If this process is adopted and approved, the net result will be to undermine the goal of cyber deterrence as enunciated in the February 2017 Defense Science Board Report. Intervals of 15 months between assessments and corrections will enable large gaps that foreign adversaries will exploit.

c. **Requirement R3.** Implementing one or more documented processes for verifying the integrity and authenticity (medium and high impact BES systems) for software and firmware would require substantial forensic competency by the utility. Further, in the reality of the sophisticated attacks that have given rise to Order No. 829, there is very little likelihood of success by over

1400 independent "responsible entities" and the potential for unreasonable expenses in the process. Or did the SDT intend to minimize the task? This illusory requirement illustrates the need for broader initiatives, both within the electric utility industry and outside the industry.

d. **Requirement R4.** The requirement for controlling vendor remote access seriously ignores many gaps and related problems In CIP v5/v6, in the categorization structure and in the process proposed. It fails to lay down hard controls on vendor access and yet requires a complex "documented" process which can easily pass table top compliance review without correcting the many holes in systems as they operate that will remain available to adversaries. Exceptions to CIP standards leave thousands of cyber assets directly interfacing with the internet, not covered by this standard as well as all others. Yet those assets are directly linked to OT and IT systems providing paths for malware, data corruption and opportunities for adversarial control, through supply chain vulnerabilities. With respect to Supply Chain vulnerabilities, Grid connectivity makes nonsense of the categorization of Cyber Assets as "low", "medium" and "high" impact.

e. The practice of rating a low impact asset as "no effect on the BES overall" has consistently ignored the sum of such assets effect on the vulnerabilities of the Grid to uncontrled separation and cascading outages, and permanent damage to long-replacement-time grid equipment.

f. **Requirement R5**. Given the holes described in **R4**, this requirement for verifying product integrity and controlling vendor accesses, and presumably unmonitored machine-to-machine accesses for the few low impact cyber assets covered by CIP standards, is intended to obscure the realities of major portals available to the nation's adversaries. FERC knows CIP standards utterly fail to address the vulnerabilities of so-called low level , so-called "Low Impact" cyber assets, as have been demonstrated to enable takedown of elements of the Ukrainian electric distribution system in both December 2015 and December 2016 . FERC knows that such assets represent major avenues for attack on the BES and the short path to "Distribution" systems and nuclear sites. Notwithstanding, the current supply chain standard needs a major overhaul to provide effective and verifiable system security.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016

Anticipated Actions	Date
45-day formal comment period with ballot	May 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Rationale for Requirement R2:
Proposed Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement as the objective of Part 2.4. The objective of Requirement R2 Part 2.5 is for entities to have the ability to rapidly disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-6 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access): • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

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

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-~~5~~6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~5~~6:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for Project 2016-03

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

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

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

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

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

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

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

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

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

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

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

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Rationale for Requirement R2:
Proposed Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement as the objective of Part 2.4. The objective of Requirement R2 Part 2.5 is for entities to have the ability to rapidly disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

R2. Each Responsible Entity ~~allowing Interactive Remote Access to BES Cyber Systems~~ shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, ~~U~~utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	• Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access): • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access. •

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

   1.3. Compliance Monitoring and Assessment Processes:

   - Compliance Audit
   - Self-Certification
   - Spot Checking
   - Compliance Investigation
   - Self-Reporting
   - Complaint

   1.4. Additional Compliance Information:

   None.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-~~5~~ 6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-~~5~~ 6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; ~~.~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-~~5~~ 6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	

6	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

CIP-005-5-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

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

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016

Anticipated Actions	Date
45-day formal comment period with ballot	May 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one

or more requirements in a NERC or Regional Reliability Standard.

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

4.2.1.4 Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and

including the first interconnection point of the starting station service of the next generation unit(s) to be started.

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the standards include the personnel risk assessment program and the personnel training

program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

Rationale for Requirement R1:
Proposed requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The 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.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	For 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.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed during the baseline change.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets

and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process to verify the identity of the software source (1.6.1) but does not have a process to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-3, Requirement R4,	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

CIP-010-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

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

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Integrity and Authenticity

The concept of verifying software integrity and authenticity is a key control in preventing the introduction of malware or counterfeit software. This 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. The intent of the SDT is to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches. That is why the requirement was not placed in CIP-007 - Security Patch Management.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware of software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid

implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless,

including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other

programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.

- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the

BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

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

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-0~~10-2~~10-3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

4.1.1 Balancing Authority

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

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

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

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

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-0~~10-2~~10-3:

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

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

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

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

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

5. Effective Dates:

See Implementation Plan for ~~CIP-010-2~~Project 2016-03.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show

documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:
Proposed requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The 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.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	For 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.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed during the baseline change.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-0~~10-2~~10-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process to verify the identity of the software source (1.6.1) but does not have a process to verify the integrity of the software provided by the software	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					source when the method to do so is available to the Responsible Entity from the software source (1.6.2)	requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6)
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days~~.~~ (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2 10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-2 10-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-2 10-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-2 10-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-2 10-3, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2 10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-2 10-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2 10-3, Requirement R4,	Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2 10-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media,	Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2 10-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 1.2. (R4)	but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~2~~10-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~2~~10-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Guideline and Technical Basis (attached).

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-2. Docket No. RM15-14-000	

3	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

CIP-0~~10-2~~10-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

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

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-0~~10-2~~10-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Integrity and Authenticity

The concept of verifying software integrity and authenticity is a key control in preventing the introduction of malware or counterfeit software. This 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. The intent of the SDT is to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches. That is why the requirement was not placed in CIP-007 - Security Patch Management.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware of software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of “per Transient Cyber Asset capability” is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g., using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they

should check the image during the build to ensure that there is not malicious software on the image.

- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.
- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent

malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that

can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

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

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010~~-2~~ and CIP-007~~-6~~ to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Standard Development Timeline

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

Description of Current Draft

This is the first draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	January 19 - March 6, 2017

Anticipated Actions	Date
45-day formal comment period with ballot	May 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

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

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

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

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

Rationale for Requirement R1:
The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES 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); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation

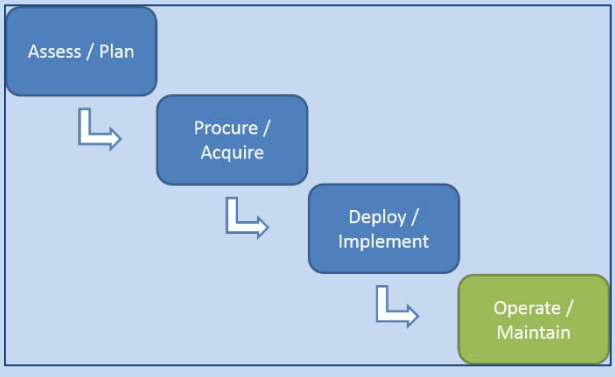
processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



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;

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).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

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.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited

to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

Rationale for Requirement R3:
The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

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. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the elements in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the elements in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2.	N/A	N/A	N/A	The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 829.	NA

Standard Attachments

None

Guidelines and Technical Basis

Rationale

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

Standard Development Timeline

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

Description of Current Draft

This is the first draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	January 19 - March 6, 2017

Anticipated Actions	Date
45-day formal comment period with ballot	May 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

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

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

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

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

Rationale for Requirement R1:
The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES 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); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation

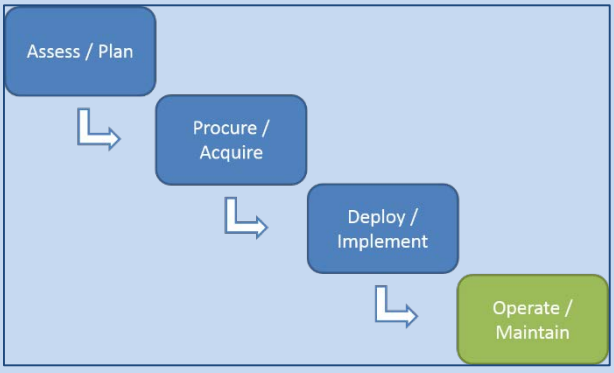
processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



R1. Each Responsible Entity shall ~~implement~~ develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. ~~that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.~~ The plan(s) shall ~~address~~include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~**1.1.** The use of controls in BES Cyber System planning and development to:~~

~~**1.1.1.** Identify and assess risk(s) during the procurement and deployment of vendor products and services; and~~

~~**1.1.2.** Evaluate methods to address identified risk(s).~~

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.**~~

~~The use of controls in procuring vendor product(s) or service(s) that address the following items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets:~~ ~~The use of~~

1.2. One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:

1.2.1. ~~Process(es) for notification of vendor security events;~~ 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;

~~**1.2.1.**~~**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;

~~**1.2.2.**~~**1.2.3.** ~~Process(es) for notification when vendor employee remote or onsite access should no longer be granted;~~ Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

~~**1.2.3.**~~**1.2.4.** ~~Process(es) for disclosure of known vulnerabilities;~~ Disclosure by vendors of known vulnerabilities;

~~**1.2.4.** Coordination of response to vendor-related cyber security incidents;~~

1.2.5. ~~Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use;~~ 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 remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and~~ Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

~~1.2.6.~~1.2.7.

~~Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.~~

M1. Evidence shall include ~~(i)~~ one or more documented supply chain cyber security risk management plan(s) ~~that address controls for mitigating cyber security risks~~ as specified in the Requirement.~~; and (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk management plan(s).~~

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1 *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*.

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.

~~M1.~~M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

Rationale for Requirement ~~R2~~R3:
The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

~~Order No. 829 also directs that the p~~Entities perform periodic assessment ~~"ensure that the required~~to keep plans ~~remains~~ up-to-date and~~,~~ address~~ing~~ current and emerging supply chain-related concerns and vulnerabilities.~~" (P. 47).~~ Examples of sources of information that the entity could consider~~s~~ include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

~~R2.~~R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval ~~update, as necessary,~~of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months~~, which shall include:~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~**2.1.** Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and~~

~~**2.2.** Obtaining CIP Senior Manager or delegate approval.~~

~~M2.~~M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s~~) and evaluation of revisions~~). ~~, if any, to address applicable new supply chain security risks and mitigation measures as specified in the Requirement.~~ Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

~~**R3.** Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*~~

~~**3.1.** Operating System(s);~~

~~**3.2.** Firmware;~~

~~**3.3.** Commercially available or open-source application software; and~~

~~**3.4.** Patches, updates, and upgrades to 3.1 through 3.3.~~

~~**M3.** Evidence shall include (i) a documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation that the entity performed the actions contained in the process to verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to installation on high and medium impact BES Cyber Systems.~~

R4. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

4.1. Authorization of remote access by the Responsible Entity;

4.2. Logging and monitoring of remote access sessions to detect unauthorized activity; and

4.3. Disabling or otherwise responding to unauthorized activity during remote access sessions.

M4. Evidence shall include (i) a documented process(es) for controlling vendor remote access as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation of authorization of vendor remote access; hard copy or electronic logs of vendor-initiated Interactive Remote Access and system-to-system remote access sessions; hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.

R5. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

5.1. Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and

5.2. Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).

M5. Evidence may include, but is not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate for each cyber security policy.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with

mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the elements in Part 1.2.1 through Part 1.2.6. ~~N/A~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the elements in Part 1.2.1 through Part 1.2.6. ~~N/A~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop ~~The Responsible Entity did not implement~~one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2.	N/A ~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.~~	N/A ~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.~~	N/A ~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.~~	The Responsible Entity did not implement its supply chain cyber security risk management plan(s) as specified in the requirement.~~The Responsible Entity did not review and update, as necessary, its supply chain cyber security risk management plan(s) and obtain CIP Senior Manager or delegate approval within 18 calendar months of the previous review as specified in the Requirement.~~
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.~~The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and~~

				~~firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.~~

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 829.	NA

Standard Attachments

None

Guidelines and Technical Basis

Rationale

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard

Applicable Standard(s)

CIP-005-6 — Cyber Security — Electronic Security Perimeters

CIP-010-3 — Configuration Change Management and Vulnerability Assessments

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

CIP-005-5 — Cyber Security — Electronic Security Perimeters

CIP-010-2 — Configuration Change Management and Vulnerability Assessments

Prerequisite Standard(s)

None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
  - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator

- Transmission Operator
- Transmission Owner

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing 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 Bulk Electric System (BES) operations. Order No. 829 (at P 2) states:

> [The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

FERC directed NERC to submit the new or modified Reliability Standard(s) within one year of the effective date of Order No. 829, i.e., by September 27, 2017.

General Considerations

Consistent with the directive to develop a forward-looking Reliability Standard, the implementation of Reliability Standards in Project 2016-03 do not require the abrogation or re-negotiation of contracts (including amendments to master agreements and purchase orders) with vendors, suppliers or other entities executed as of the effective date of the proposed Reliability Standards (See FERC Order No. 829, P. 36).

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

Effective Date

For all Reliability Standards in Project 2016-03 — CIP-005-6, CIP-010-3, and CIP-013-1
Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date

the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

CIP-013-1 Requirement R3
The initial review and approval of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement R3 must be completed on or before the effective date of CIP-013-1.

Definition

None

Retirement Date

Standards listed in the **Requested Retirement(s)** section shall be retired immediately prior to the effective date in the particular jurisdiction in which the revised standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard ~~CIP-013-1~~

Applicable Standard(s)

CIP-005-6 — Cyber Security — Electronic Security Perimeters

CIP-010-3 — Configuration Change Management and Vulnerability Assessments

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

CIP-005-5 — Cyber Security — Electronic Security Perimeters

CIP-010-2 — Configuration Change Management and Vulnerability Assessments~~None~~

Prerequisite Standard(s)

None

Applicable Entities

~~**CIP-013-1 — Cyber Security — Supply Chain Risk Management**~~

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
  - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner

- Reliability Coordinator
- Transmission Operator
- Transmission Owner

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing 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 Bulk Electric System (BES) operations. Order No. 829 (at P 2) states:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

FERC directed NERC to submit the new or modified Reliability Standard(s) within one year of the effective date of Order No. 829, i.e., by September 27, 2017.

General Considerations

Consistent with the directive to develop a forward-looking Reliability Standard, the implementation of ~~r~~Reliability ~~s~~Standards in Project 2016-03 ~~CIP-013-1~~ do~~es~~ not require the abrogation or re-negotiation of contracts (including amendments to master agreements and purchase orders) with vendors, suppliers or other entities executed as of the effective date of the proposed Reliability ~~s~~Standards~~CIP-013-1~~ (See FERC Order No. 829, P. 36).

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

Effective Date

~~CIP-013-1 — Cyber Security — Supply Chain Risk Management~~For all Reliability ~~s~~Standards in Project 2016-03 — CIP-005-6, CIP-010-3, and CIP-013-1

Where approval by an applicable governmental authority is required, the Reliability ~~standards~~ Standards ~~s~~ shall become effective on the first day of the first calendar quarter that is ~~twelve (12~~18~~)~~ months after the effective date of the applicable governmental authority's order approving the

Reliability ~~standards~~Standards~~s~~, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability ~~standards~~ Standards~~s~~ shall become effective on the first day of the first calendar quarter that is ~~twelve (12~~18~~)~~ months after the date the Reliability ~~standards~~ Standards~~s~~ is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

CIP-013-1 Requirement ~~R2~~R3

The initial review and approval ~~and update, as necessary,~~ of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement ~~R2~~ R3 must be completed on or before ~~within fifteen (15) calendar months of~~ the effective date of CIP-013-1.

Definition

None

Retirement Date

Standards listed in the **Requested Retirement(s)** section shall be retired immediately prior to the effective date in the particular jurisdiction in which the revised standards are becoming effective.~~None~~

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Unofficial Comment Form

Project 2016-03 Cyber Security Supply Chain Risk Management

DO NOT use this form for submitting comments. Use the electronic form to submit comments on the following proposed standards:

- CIP-013-1 – Cyber Security – Supply Chain Risk Management
- CIP-005-6 – Cyber Security – Electronic Security Perimeter(s)
- CIP-010-3 – Cyber Security – Configuration Change Management and Vulnerability Assessments

The electronic comment form must be completed by **8:00 p.m. Eastern, Thursday, June 15, 2017**.

Documents and information about this project are available on the project page. If you have any questions, contact Senior Standards Developer, Mark Olson (via email), or at (404) 446-9760.

Background Information

On July 21, 2016, the Federal Energy Regulatory Commission (Commission) issued Order No. 829 directing 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 Bulk Electric System (BES) operations as follows:

> "[The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."

NERC must file the new or revised Standard by September 27, 2017, to meet the one-year deadline established by the Commission in Order No. 829.

The standard drafting team (SDT) has developed the proposed standard and modifications to approved standards to address the above directives.

Questions

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

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on

supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☐ Yes
☐ No
Comments:

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☐ Yes
☐ No
Comments:

9. Provide any additional comments for the SDT to consider, if desired.
Comments:

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-03 — Cyber Security — Supply Chain Risk Management

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **Project 2016-03 — Cyber Security — Supply Chain Risk Management.** Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines. The Cyber Security Supply Chain Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement

A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in an Operations Planning time horizon to develop one or more documented supply chain cyber security risk management plan(s). If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective, which is to address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-013-1, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the elements in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the elements in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to develop one or more documented supply chain cyber security risk management plan(s) that set forth the controls.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in Operations Planning time horizon that requires entities to implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. If violated, failing to implement this plan could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R2			
Lower	**Moderate**	**High**	**Severe**
N/A	N/A	N/A	The Responsible Entity did not implement its supply chain cyber security risk management plan(s) as specified in the requirement.

VSL Justifications for CIP-013-1, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R2 is SEVERE which is consistent with binary criteria. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSL is based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	A single VSL of Severe is assigned.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	R3 is a requirement in Operations Planning time horizon that requires the Responsible Entity to periodically review and obtain CIP Senior Manager or delegate approval of supply chain cyber security risk management plans. The reliability objective is to ensure plans remain up to date and address current and emerging supply chain-related cyber security concerns and vulnerabilities. If the requirement is violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R3 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of the review requirement by some number of months less than 18 calendar months does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-005-6, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in an Operations Planning and Same Day Operations time horizon to implement one or more documented processes for controlling vendor remote access to high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with the addition of two parts addressing specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-005-6, R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

VSL Justifications for CIP-005-6, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.

FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R2 is not binary. Guideline 2b: The proposed VSLs do not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.

Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in Operations Planning time horizon that requires the Responsible Entity to implement one or more documented processes that include each of the applicable requirement parts for configuration change management. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with an additional part to address specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation

VSLs for CIP-010-3, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ;	The Responsible Entity has not documented or implemented any configuration change management process(es) (R1); ; OR

		OR The Responsible Entity has The Responsible Entity has a process to verify the identity of the software source (1.6.1) but does not have a process to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6.2).	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1); . OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration (1.2); OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration (1.3); OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from

			the existing baseline configuration (1.4.1); OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change (1.4.2 & 1.4.3); OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration (1.5.1); OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and

			production environments (1.5.2); OR The Responsible Entity does not have a process to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6).

VSL Justifications for CIP-010-3, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-010-3, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-03 — Cyber Security — Supply Chain Risk Management

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **Project 2016-03 — Cyber Security — Supply Chain Risk Management.** Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines. The Cyber Security Supply Chain Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in an Operations Planning time ~~frame~~ horizon to develop one or more documented supply chain cyber security risk management plan(s). If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective, which is to address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle~~develop one or more documented supply chain cyber security risk management plan(s)~~. Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-013-1, R1			
Lower	Moderate	High	Severe

The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the elements in Part 1.2.1 through Part 1.2.6.~~N/A~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the elements in Part 1.2.1 through Part 1.2.6.~~N/A~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.~~The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include one of the elements specified in Parts 1.1 or 1.2.~~	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of processes in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop ~~The Responsible Entity did not implement~~one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.~~The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include either of the elements specified in Parts 1.1 or 1.2.;~~ ~~OR~~ ~~The Responsible Entity did not implement one or more~~

			~~documented supply chain risk management plan(s) as specified in the Requirement.~~

VRF Justifications for CIP-013-1, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VRF Justifications for CIP-013-1, R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to develop one or more documented supply chain cyber security risk management plan(s) that set forth the controls.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in Operations Planning time ~~frame~~ horizon that requires entities to implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. If violated, failing to implement this plan could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R2			
Lower	**Moderate**	**High**	**Severe**
~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.~~N/A	~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.~~N/A	~~The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.~~N/A	The Responsible Entity did not implement its supply chain cyber security risk management plan(s) as specified in the requirement.~~The Responsible Entity did not review and update, as necessary, its supply chain cyber security risk management plan(s) and obtain CIP Senior Manager or delegate approval within 18 calendar months of the previous review as specified in the Requirement.~~

VSL Justifications for CIP-013-1, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R2 is SEVERE which is consistent with ~~not~~ binary criteria. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-013-1, R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSL~~s are~~ is based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	~~An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.~~ A single VSL of Severe is assigned.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	R3 is a requirement in Operations Planning time ~~frame~~ horizon that requires the Responsible Entity to ~~perform~~ periodically review and obtain CIP Senior Manager or delegate approval of supply chain cyber security risk management plans. ~~implement one or more documented process(es) for software integrity and authenticity controls to address risks from compromised software and firmware on high and medium impact BES Cyber Systems.~~ The reliability objective is to ensure plans remain up to date and address current and emerging supply chain-related cyber security concerns and vulnerabilities. If the requirement is violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of ~~a the~~the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation**

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
	R3 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.~~N/A~~	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.~~The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.~~

VSL Justifications for CIP-013-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. ~~The VSL assignment for R4 is Severe which is consistent with binary criteria.~~ Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-013-1, R3	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of the review requirement by some number of months less than 18 calendar months does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.~~Only a Severe VSL is assigned.~~
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-~~013~~005-~~01~~06, ~~R4~~R2	
Proposed VRF	**Medium**
NERC VRF Discussion	~~R4~~ R2 is a requirement in an Operations Planning and Same Day Operations time ~~frame~~ horizon to implement one or more documented process~~(es)~~es for controlling vendor remote access to high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of ~~a~~ the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a ~~new~~ revised requirement with the addition of two parts addressing specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** ~~R4~~ R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-~~013~~005-~~1~~6, ~~R4~~R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.~~N/A~~	The Responsible Entity did not implement~~ed one or more documented~~ process~~(es)~~es for one of the applicable items for Requirement Parts 2.1 through 2.3~~controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include one of the elements specified in Part 4.1 through Part 4.3~~.	The Responsible Entity did not implement~~ed one or more documented~~ process~~(es)~~es for two of the applicable items for Requirement Parts 2.1 through 2.3~~controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include two of the elements specified in Part 4.1 through Part 4.3~~.	The Responsible Entity did not implement~~ed one or more documented~~ process~~(es)~~es for three of the applicable items for Requirement Parts 2.1 through 2.3; ~~controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include any of the elements specified in Part 4.1 through Part 4.3;~~ OR The Responsible Entity did not have~~implement~~ one or more ~~documented process(es)~~methods for determining active ~~controlling~~ vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) ~~to high and medium impact BES Cyber Systems as specified in the Requirement~~and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

VSL Justifications for CIP-~~013005~~-~~16~~, ~~R4~~R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for ~~R4~~ R2 is not binary. Guideline 2b: The proposed VSLs do not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-~~013005~~-~~16~~, ~~R4~~R2	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-~~013~~010-1, ~~R5~~R1	
Proposed VRF	**~~Lower~~Medium**
NERC VRF Discussion	~~R5~~ R1 is a requirement in Operations Planning time ~~frame~~ horizon that requires the Responsible Entity to implement one or more documented processes that include each of the applicable requirement parts for configuration change management. ~~with at least one asset identified in CIP-002 containing low impact BES Cyber Systems to have one or more documented cyber security policies to address software integrity and authenticity and vendor remote access for its low impact BES Cyber Systems. If violated, it would not, under the emergency, abnormal, or restorative conditions anticipated by the policies, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system.~~ If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a ~~new~~ revised requirement with an additional part to address~~ing~~ specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of ~~Lower~~ Medium is consistent with the NERC VRF definition as discussed above.

VRF Justifications for CIP-~~013~~010-1, ~~R5~~R1	
Proposed VRF	~~Lower~~Medium
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** ~~R5~~ R1 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation

VSLs for CIP-~~013~~010-~~1~~3, ~~R5~~R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity ~~had~~ has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review~~.	The Responsible Entity ~~had~~ has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 16 calendar months but less than or equal to 17 calendar months from the previous review~~.	The Responsible Entity ~~had~~ has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include one of the elements in Parts 5.1 or 5.2~~; OR The Responsible Entity ~~had~~ has The Responsible Entity has a	The Responsible Entity ~~had~~ has not documented or implemented any configuration change management process(es) (R1); ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include either of the elements in Parts 5.1 or 5.2~~; OR The Responsible Entity ~~had~~ has documented and implemented a configuration change

		process to verify the identity of the software source (1.6.1) but does not have a process to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6.2).~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 17 calendar months but less than or equal to 18 calendar months from the previous review.~~	management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1); ~~cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review~~. OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration (1.2); OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration (1.3); OR

			The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration (1.4.1); OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change (1.4.2 & 1.4.3); OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration (1.5.1); OR

			The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments (1.5.2); OR The Responsible Entity does not have a process to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source (1.6).

VSL Justifications for CIP-~~013~~010-~~1~~3, ~~R5~~R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for ~~R5~~ R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.

VSL Justifications for CIP-~~013~~010-~~1~~3, ~~R5~~R1	
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

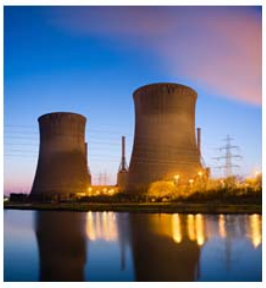
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-1

RELIABILITY | ACCOUNTABILITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Reliability Standard **CIP-013-1 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1].

This implementation guidance provides considerations for implementing the requirements in CIP-013-1 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-1. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

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:*

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;*

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).*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security 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 terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is 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.

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.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security 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 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 the Responsible Entities 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.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-3, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

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:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". 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. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

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).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:

- Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
- Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

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;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

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;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

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*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

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

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

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

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.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

Requirement R3

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.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) “Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation”
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - “Cybersecurity Procurement Language for Energy Delivery Systems”

Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified 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.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.* CIP-013-1 is applicable to high and medium impact BES Cyber Systems. The proposed applicability appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations.
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed/modified standard(s) must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., the Reliability Standard should set goals (the	The directive is addressed by Requirements R1, R2, and R3 of proposed CIP-013-1. Requirement R1 specifies that entities must develop, and Requirement R2 specifies that entities must implement, one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems that include one or more process(es) for mitigating

Order No. 829 Citation	Directive / Guidance	Resolution
	"what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how")).	cyber security risks to BES Cyber Systems. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle. **Proposed CIP-013-1 Requirement R1** **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: **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;

Order No. 829 Citation	Directive / Guidance	Resolution
		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; **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). **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require 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. This periodic assessment should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	The directive is addressed in proposed CIP-013-1 Requirement R3. **Proposed CIP-013-1 Requirement R3** **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
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the	The directive is addressed in proposed CIP-013-1 Requirement R3 (shown above) and supporting guidance.

Order No. 829 Citation	Directive / Guidance	Resolution
	responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	**Proposed CIP-013-1 Rationale for Requirement R3:** Entities perform periodic assessment to keep plans up-to-date and, addressing current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC) *Implementation Guidance* developed by the drafting team and submitted for ERO endorsement includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and CIP-010-3 Requirements R1 Part 1.6. The 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. **Proposed CIP-010-3 Requirement R1** **R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. **1.6.** For 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:

Order No. 829 Citation	Directive / Guidance	Resolution
		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.
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5. The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. The objective of Requirement R2 Part 2.5 is for entities to have the ability to rapidly disable active remote access sessions in the event of a system breach. **Proposed CIP-005-6 Requirement R2** **R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-6 Table R2 –Remote Access Management.: **2.4** Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Order No. 829 Citation	Directive / Guidance	Resolution
		2.5 Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by CIP-005-6 Requirement R2 Part 2.5 (above).
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address 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. 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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).
Objective 4: Vendor Risk Management and Procurement Controls		
P 59	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. Specifically, NERC must address controls for the following topics: (1) vendor security event notification processes; (2) vendor personnel termination 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. NERC should also	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).

Order No. 829 Citation	Directive / Guidance	Resolution
	consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	

Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified 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.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.* CIP-013-1 is applicable to high and medium impact BES Cyber Systems. The proposed applicability appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations.
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed/modified standard(s) must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., the Reliability Standard should set goals (the	The directive is addressed by Requirements R1, ~~R3~~R2, ~~R4,~~ and ~~R5~~ R3 of proposed CIP-013-1. Requirement R1 specifies that entities must ~~implement~~ develop, and Requirement R2 specifies that entities must implement, one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems that ~~address~~ include one or more

Order No. 829 Citation	Directive / Guidance	Resolution
	"what"), while allowing flexibility in how a responsible entity subject to the Reliability Standard achieves that goal (the "how")).	process(es)~~controls~~ for mitigating cyber security risks to BES Cyber Systems ~~and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets~~. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle. ~~Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle as described further below.~~ **Proposed CIP-013-1 Requirement R1** **R1.** Each Responsible Entity shall ~~implement~~ develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. ~~that address controls for mitigating cyber security risks to BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets.~~ The plan(s) shall ~~address~~include: ~~**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

Order No. 829 Citation	Directive / Guidance	Resolution
		vendor(s)~~One or more process(es) used The use of controls 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; (ii) network architecture security; and (iii) transitions from one vendor(s) to another vendor(s). planning and development to:~~ ~~**1.2.** Identify and assess risk(s) during the procurement and deployment of vendor products and services; and~~ ~~**1.3.**1.1. Evaluate methods to address identified risk(s).~~ ~~**1.4.**1.2. One or more process(es) used in procuring BES Cyber Systems ~~The use of controls in procuring vendor product(s) or service(s)~~ that address the following, as applicable~~ items, to the extent each item applies to the Responsible Entity's BES Cyber Systems and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets~~: **1.2.1.** ~~Process(es) for n~~Notification by the ~~of~~ 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~~events~~;

Order No. 829 Citation	Directive / Guidance	Resolution
		~~1.4.1.~~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; ~~1.4.2.~~1.2.3. ~~Process(es) for n~~Notification by vendors when ~~vendor employee~~ remote or onsite access should no longer be granted to vendor representatives; ~~1.4.3.~~1.2.4. ~~Process(es) for d~~Disclosure by vendors of known vulnerabilities; ~~1.4.4. Coordination of response to vendor-related cyber security incidents;~~ ~~1.4.5.~~1.2.5. ~~Process(es) for verifying~~Verification of software integrity and authenticity of all software and patches provided by the vendor ~~that are intended~~ for use in the BES Cyber System; and ~~1.4.6.~~1.2.6. Coordination of ~~remote access~~ controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)~~; and Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable~~. **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

Order No. 829 Citation	Directive / Guidance	Resolution
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require 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. This periodic assessment should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	The directive is addressed in proposed CIP-013-1 Requirement ~~R2~~R3. **Proposed CIP-013-1 Requirement ~~R2~~R3** **~~R2~~R3.** Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of ~~update, as necessary,~~ its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months~~, which shall include:~~ ~~**2.1.** Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and~~ ~~**2.2.** Obtaining CIP Senior Manager or delegate approval.~~
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	The directive is addressed in proposed CIP-013-1 Requirement ~~R2~~ R3 ~~part 2.1~~ (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement ~~R2~~R3:** ~~Order No. 829 also directs that the~~Entities perform periodic assessment ~~"ensure that the required~~to keep plans ~~remains~~ up-to-date and, addressing current and emerging supply chain-related concerns and vulnerabilities~~" (P. 47)~~. Examples of sources of information that the entity could consider~~s~~ include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC)

Order No. 829 Citation	Directive / Guidance	Resolution
		~~*Technical Guidance and Examples*~~*Implementation Guidance* ~~document~~ developed by the drafting team and submitted for ERO endorsement includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and CIP-010-3 Requirements ~~R3~~ R1 ~~and R5~~ Part 1.6~~5.1~~. ~~CIP-013-1 Requirement R3 applies to high and medium impact BES Cyber Systems.~~ The 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. **Proposed CIP-~~013~~010-~~1~~ 3 Requirement ~~R3~~R1** **R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*.~~Each Responsible Entity shall implement one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems:~~ **1.6.** For 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

Order No. 829 Citation	Directive / Guidance	Resolution
		1.6.2. Verify the integrity of the software obtained from the software source.~~Operating System(s);~~ ~~**3.1.** Firmware;~~ ~~**3.2.** Commercially available or open-source application software; and~~ ~~**3.3.** Patches, updates, and upgrades to 3.1 through 3.3.~~ ~~**Proposed CIP-013-1 Requirement R5**~~ ~~**R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:~~ ~~**5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and...~~
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-~~013~~005-~~1~~6 Requirement ~~R4~~ R2 Parts ~~4.1~~2.4 and ~~4.2~~2.5. The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.~~ and Requirement R5 Part 5.2. Requirement R4 applies to high and medium impact BES Cyber Systems.~~

Order No. 829 Citation	Directive / Guidance	Resolution
		~~Requirement R5 applies to low impact BES Cyber Systems.~~ The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. The objective of Requirement R2 Part 2.5 is for entities to have the ability to rapidly disable active remote access sessions in the event of a system breach. **Proposed CIP-~~013~~005-~~1~~ 6 Requirement ~~R4~~R2** **R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-6 Table R2 –Remote Access Management.~~Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s)~~: ~~**4.1.** Authorization of remote access by the Responsible Entity;~~ ~~**4.2.** Logging and monitoring of remote access sessions to detect unauthorized activity; and~~ ~~**4.3.** Disabling or otherwise responding to unauthorized activity during remote access sessions.~~

Order No. 829 Citation	Directive / Guidance	Resolution
		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). ~~**Proposed CIP-013-1 Requirement R5**~~ ~~**R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems:~~ ~~**5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).~~
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by CIP-005-6 Requirement ~~R4~~ R2 Part ~~4~~2.~~3~~ 45 (above) ~~and Requirement R5 Part 5.2 (above)~~.
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address a responsible entity's CIP Senior Manager's (or delegate's) identification and documentation of the risks of proposed information system planning and system	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).

Order No. 829 Citation	Directive / Guidance	Resolution
	development actions. 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.	
Objective 4: Vendor Risk Management and Procurement Controls		
P 59	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. Specifically, NERC must address controls for the following topics: (1) vendor security event notification processes; (2) vendor personnel termination 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. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-03 Cyber Security Supply Chain Risk Management CIP-005-6, CIP-010-3 and CIP-013-1

Formal Comment Period Open through June 15, 2017
Ballot Pools Open for Additional Members through May 31, 2017

Now Available

A 45-day formal comment period will be open through **8 p.m. Eastern, Thursday, June 15, 2017** for the following standards:

1. **CIP-005-6 - Cyber Security – Electronic Security Perimeter(s);**
2. **CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments;** and
3. **CIP-013-1 – Cyber Security – Supply Chain Risk Management**.

The standard drafting team's considerations of the responses received from the last comment period are reflected in the proposed standards.

Commenting

Use the electronic form to submit comments on the standard. If you experience any difficulties using the electronic form, contact Nasheema Santos An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

The existing CIP-013-1 ballot pool was used for all of the ballots associated with this project. The ballot pools for CIP-005-6 and CIP-010-3 have been opened to allow stakeholders to join if they are not existing members. The ballot pools are open through **8 p.m. Eastern, Wednesday, May 31, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for CIP-005-6 and CIP-010-3, an additional ballot for CIP-013-1 as well as the non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **June 6-15, 2017**.

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

For more information or assistance, contact Senior Standards Developer, Mark Olson (via email), or at (404) 446-9760.

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

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/92)
Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-005-6 IN 1 ST
Voting Start Date: 6/6/2017 12:01:00 AM
Voting End Date: 6/15/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 298
Total Ballot Pool: 391
Quorum: 76.21
Weighted Segment Value: 89.84

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	101	1	66	0.868	10	0.132	0	2	23
Segment: 2	7	0.6	5	0.5	1	0.1	0	0	1
Segment: 3	88	1	58	0.906	6	0.094	0	2	22
Segment: 4	24	1	15	0.882	2	0.118	0	2	5
Segment: 5	92	1	54	0.871	8	0.129	0	4	26
Segment: 6	62	1	47	0.922	4	0.078	0	1	10
Segment: 7	3	0.1	1	0.1	0	0	0	2	0
Segment: 8	4	0.1	1	0.1	0	0	0	0	3
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	9	0.5	5	0.5	0	0	0	1	3

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	391	6.4	253	5.75	31	0.65	0	14	93

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Negative	Comments Submitted
1	AES - Dayton Power and Light Co.	Hertzel Shamash		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		None	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	CPS Energy	Glenn Pressler		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		None	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	VELCO -Vermont Electric Power Company, Inc.	Randy Buswell		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	ISO New England, Inc.	Michael Puscas		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	AEP	Aaron Austin		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Affirmative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		None	N/A
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		None	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Darl Shimko		Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Mick Neshem		Affirmative	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Austin Energy	Esther Weekes		None	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	LaGen	Richard Comeaux		Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Abstain	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Austin Energy	Jeanie Doty		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Dynegy Inc.	Dan Roethemeyer		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		None	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	MGE Energy - Madison Gas and Electric Co.	Steven Schultz		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Abstain	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Comments Submitted
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Abstain	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons	Amy Casuscelli	Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	MGE Energy - Madison Gas and Electric Co.	Robert Thorson		None	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Abstain	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara	Luiggi Beretta	Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southeastern Power Administration	Douglas Spencer		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Abstain	N/A
8	David Kiguel	David Kiguel		None	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		None	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		None	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 391 of 391 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/92)
Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-010-3 IN 1 ST
Voting Start Date: 6/6/2017 12:01:00 AM
Voting End Date: 6/15/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 298
Total Ballot Pool: 391
Quorum: 76.21
Weighted Segment Value: 82.92

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	101	1	63	0.829	13	0.171	0	2	23
Segment: 2	7	0.6	3	0.3	3	0.3	0	0	1
Segment: 3	88	1	54	0.844	10	0.156	0	2	22
Segment: 4	24	1	15	0.882	2	0.118	0	2	5
Segment: 5	92	1	50	0.806	12	0.194	0	4	26
Segment: 6	62	1	44	0.863	7	0.137	0	1	10
Segment: 7	3	0.1	1	0.1	0	0	0	2	0
Segment: 8	4	0.1	1	0.1	0	0	0	0	3
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	9	0.4	4	0.4	0	0	0	2	3

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	391	6.3	236	5.224	47	1.076	0	15	93

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Negative	Comments Submitted
1	AES - Dayton Power and Light Co.	Hertzel Shamash		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Negative	Comments Submitted
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		None	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	Third-Party Comments
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	CPS Energy	Glenn Pressler		Negative	Third-Party Comments
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Third-Party Comments
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	VELCO -Vermont Electric Power Company, Inc.	Randy Buswell		Affirmative	N/A
1	Westar Energy	Kevin Giles		Negative	Third-Party Comments
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Negative	Comments Submitted
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	ISO New England, Inc.	Michael Puscas		Negative	Third-Party Comments
2	Midcontinent ISO, Inc.	Terry Bllke		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Aaron Austin		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		None	N/A
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		None	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		None	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Darl Shimko		Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Mick Neshem		Negative	Comments Submitted
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Negative	Third-Party Comments
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Austin Energy	Esther Weekes		None	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	LaGen	Richard Comeaux		Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Abstain	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Austin Energy	Jeanie Doty		None	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	Third-Party Comments
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		Negative	Third-Party Comments
5	Dairyland Power Cooperative	Tommy Drea		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Dynegy Inc.	Dan Roethemeyer		Abstain	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		None	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	MGE Energy - Madison Gas and Electric Co.	Steven Schultz		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Abstain	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Comments Submitted
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Abstain	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Negative	Third-Party Comments
5	Xcel Energy, Inc.	David Lemmons	Amy Casuscelli	Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	MGE Energy - Madison Gas and Electric Co.	Robert Thorson		None	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Abstain	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Negative	Third-Party Comments
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara	Luiggi Beretta	Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southeastern Power Administration	Douglas Spencer		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
7	Oxy - Occidental Chemical	Venona Greaff		Abstain	N/A
8	David Kiguel	David Kiguel		None	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		None	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	David Greene		None	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 391 of 391 entries

BALLOT RESULTS

Comment: View Comment Results (/CommentResults/Index/92)
Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 AB 2 ST
Voting Start Date: 6/6/2017 12:01:00 AM
Voting End Date: 6/15/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 288
Total Ballot Pool: 373
Quorum: 77.21
Weighted Segment Value: 88.64

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	96	1	64	0.877	9	0.123	0	2	21
Segment: 2	7	0.6	5	0.5	1	0.1	0	0	1
Segment: 3	82	1	52	0.897	6	0.103	0	2	22
Segment: 4	24	1	16	0.842	3	0.158	0	1	4
Segment: 5	87	1	51	0.85	9	0.15	0	2	25
Segment: 6	61	1	46	0.885	6	0.115	0	1	8
Segment: 7	3	0.3	3	0.3	0	0	0	0	0
Segment: 8	4	0.1	1	0.1	0	0	0	0	3
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	8	0.5	5	0.5	0	0	0	2	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	373	6.6	244	5.85	34	0.75	0	10	85

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Patricia Robertson		Negative	Comments Submitted
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	CPS Energy	Glenn Pressler		Affirmative	N/A
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	Comments Submitted
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Third-Party Comments
1	Lincoln Electric System	Danny Pudenz		None	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	Comments Submitted
1	Network and Security Technologies	Nicholas Lauriat		Negative	Comments Submitted
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		Negative	Comments Submitted
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Negative	Comments Submitted
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	Comments Submitted
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	ISO New England, Inc.	Michael Puscas		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	Comments Submitted
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		None	N/A
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		None	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		None	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Nebraska Public Power District	Tony Eddleman		Negative	Comments Submitted
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		None	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Public Utility District No. 1 of Chelan County	Mick Neshem		Negative	Comments Submitted
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	Comments Submitted
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Austin Energy	Esther Weekes		None	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Affirmative	N/A
4	LaGen	Richard Comeaux		Negative	Third-Party Comments
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Negative	Comments Submitted
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Abstain	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Austin Energy	Jeanie Doty		None	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	Comments Submitted
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		Negative	Third-Party Comments
5	Lincoln Electric System	Kayleigh Wilkerson		None	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		None	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Abstain	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	Comments Submitted
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Negative	Comments Submitted
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	Comments Submitted
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Negative	Comments Submitted
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons	Amy Casuscelli	Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	Third-Party Comments
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Abstain	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Negative	Third-Party Comments
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	Comments Submitted
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Negative	Comments Submitted
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Santee Cooper	Michael Brown		Negative	Comments Submitted
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southeastern Power Administration	Douglas Spencer		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Affirmative	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Affirmative	N/A
8	David Kiguel	David Kiguel		None	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	David Greene		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 373 of 373 entries

BALLOT RESULTS

Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-005-6 Non-binding Poll IN 1 NB
Voting Start Date: 6/6/2017 12:01:00 AM
Voting End Date: 6/16/2017 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 281
Total Ballot Pool: 369
Quorum: 76.15
Weighted Segment Value: 88.53

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	93	1	47	0.87	7	0.13	17	22
Segment: 2	7	0.5	4	0.4	1	0.1	2	0
Segment: 3	85	1	47	0.904	5	0.096	14	19
Segment: 4	23	1	10	0.769	3	0.231	4	6
Segment: 5	87	1	40	0.889	5	0.111	14	28
Segment: 6	57	1	33	0.892	4	0.108	9	11
Segment: 7	3	0.1	1	0.1	0	0	2	0
Segment: 8	4	0.3	3	0.3	0	0	0	1
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	9	0.7	7	0.7	0	0	1	1
Totals:	369	6.7	193	5.924	25	0.776	63	88

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Negative	Comments Submitted
1	AES - Dayton Power and Light Co.	Hertzel Shamash		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Abstain	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	CPS Energy	Glenn Pressler		Negative	Comments Submitted
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Abstain	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Western Energy	Kevin Giles		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Western Area Power Administration	sean erickson		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Abstain	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		Affirmative	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Austin Energy	Esther Weekes		None	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Keys Energy Services	Jeffrey Partington	Brandon McCormick	Affirmative	N/A
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Abstain	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Abstain	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Abstain	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Dynegy Inc.	Dan Roethemeyer		Abstain	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	MGE Energy - Madison Gas and Electric Co.	Steven Schultz		Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Abstain	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	None	N/A
5	SunPower	Bradley Collard		Abstain	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Tri-State G and T Association, Inc.	Mark Stein		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Abstain	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	MGE Energy - Madison Gas and Electric Co.	Robert Thorson		None	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara	Luiggi Beretta	Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		Abstain	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 369 of 369 entries

BALLOT RESULTS

Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-010-3 Non-binding Poll IN 1 NB
Voting Start Date: 6/6/2017 12:01:00 AM
Voting End Date: 6/16/2017 8:00:00 PM
Ballot Type: NB
Ballot Activity: IN
Ballot Series: 1
Total # Votes: 280
Total Ballot Pool: 367
Quorum: 76.29
Weighted Segment Value: 88.02

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	93	1	47	0.87	7	0.13	17	22
Segment: 2	7	0.5	3	0.3	2	0.2	2	0
Segment: 3	85	1	46	0.885	6	0.115	14	19
Segment: 4	22	1	9	0.75	3	0.25	4	6
Segment: 5	86	1	41	0.911	4	0.089	14	27
Segment: 6	57	1	33	0.892	4	0.108	9	11
Segment: 7	3	0.1	1	0.1	0	0	2	0
Segment: 8	4	0.3	3	0.3	0	0	0	1
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	9	0.7	7	0.7	0	0	1	1
Totals:	367	6.7	191	5.808	26	0.892	63	87

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Negative	Comments Submitted
1	AES - Dayton Power and Light Co.	Hertzel Shamash		Affirmative	N/A
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		None	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Abstain	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	CPS Energy	Glenn Pressler		Negative	Comments Submitted
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Doug Hils		Negative	Comments Submitted
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A
1	Network and Security Technologies	Nicholas Lauriat		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Abstain	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	Westar Energy	Kevin Giles		Negative	Comments Submitted
1	Western Area Power Administration	sean erickson		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		Negative	Comments Submitted
2	Midcontinent ISO, Inc.	Terry BIlke		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	AEP	Aaron Austin		Negative	Comments Submitted
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		None	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Abstain	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	Comments Submitted
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		Affirmative	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Negative	Comments Submitted
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Austin Energy	Esther Weekes		None	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Abstain	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Abstain	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CPS Energy	Robert Stevens		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Dynegy Inc.	Dan Roethemeyer		Abstain	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		None	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	MGE Energy - Madison Gas and Electric Co.	Steven Schultz		Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Abstain	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	None	N/A
5	SunPower	Bradley Collard		Abstain	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Abstain	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	Comments Submitted
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	MGE Energy - Madison Gas and Electric Co.	Robert Thorson		None	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara	Luiggi Beretta	Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		Abstain	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 367 of 367 entries

BALLOT RESULTS

Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 Non-binding Poll AB 2 NB
Voting Start Date: 6/6/2017 12:01:00 AM
Voting End Date: 6/16/2017 8:00:00 PM
Ballot Type: NB
Ballot Activity: AB
Ballot Series: 2
Total # Votes: 268
Total Ballot Pool: 351
Quorum: 76.35
Weighted Segment Value: 89.57

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes	Negative Fraction	Abstain	No Vote
Segment: 1	89	1	47	0.904	5	0.096	16	21
Segment: 2	7	0.5	4	0.4	1	0.1	2	0
Segment: 3	80	1	45	0.938	3	0.063	13	19
Segment: 4	22	1	9	0.75	3	0.25	4	6
Segment: 5	81	1	39	0.867	6	0.133	11	25
Segment: 6	56	1	32	0.889	4	0.111	9	11
Segment: 7	3	0.2	2	0.2	0	0	1	0
Segment: 8	4	0.3	3	0.3	0	0	0	1
Segment: 9	1	0.1	1	0.1	0	0	0	0
Segment: 10	8	0.7	7	0.7	0	0	1	0
Totals:	351	6.8	189	6.047	22	0.753	57	83

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	paul johnson		Negative	Comments Submitted
1	Ameren - Ameren Services	Eric Scott		Abstain	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Bryan Cox	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A
1	BC Hydro and Power Authority	Patricia Robertson		Abstain	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Devin Elverdi		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	CPS Energy	Glenn Pressler		Affirmative	N/A
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Abstain	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Abstain	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Abstain	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		None	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	Comments Submitted
1	Lincoln Electric System	Danny Pudenz		Abstain	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		None	N/A
1	M and A Electric Power Cooperative	William Price		Affirmative	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Abstain	N/A
1	Nebraska Public Power District	Jamison Cawley		Abstain	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Network and Security Technologies	Nicholas Lauriat		Abstain	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	Comments Submitted
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		None	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Abstain	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Abstain	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		None	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Abstain	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Abstain	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	Comments Submitted
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	None	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		Affirmative	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	Comments Submitted
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Abstain	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
2	Independent Electricity System Operator	Leonard Kula		Affirmative	N/A
2	ISO New England, Inc.	Michael Puscas		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Abstain	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Abstain	N/A
3	Ameren - Ameren Services	David Jendras		Abstain	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Faramarz Amjadi		Abstain	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		Affirmative	N/A
3	City of Farmington	Linda Jacobson-Quinn		None	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Affirmative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Affirmative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Clark Public Utilities	Jack Stamper		None	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Abstain	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Abstain	N/A
3	FirstEnergy - FirstEnergy Corporation	Theresa Ciancio		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Affirmative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Affirmative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Lakeland Electric	David Hadzima		None	N/A
3	Lincoln Electric System	Jason Fortik		Abstain	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		Affirmative	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Abstain	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Abstain	N/A
3	Nebraska Public Power District	Tony Eddleman		Abstain	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	Comments Submitted
3	NW Electric Power Cooperative, Inc.	John Stickley		None	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		None	N/A
3	Pacific Gas and Electric Company	John Hagen		None	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources	Michael Mertz		Abstain	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		None	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Abstain	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Abstain	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		Affirmative	N/A
3	Seattle City Light	Tuan Tran		Negative	Comments Submitted
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	Comments Submitted
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	TECO - Tampa Electric Co.	Ronald Donahey		None	N/A
3	Tennessee Valley Authority	Ian Grant		Abstain	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Abstain	N/A
4	Alliant Energy Corporation Services, Inc.	Kenneth Goldsmith		Affirmative	N/A
4	Austin Energy	Esther Weekes		None	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Affirmative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Affirmative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Bob Thomas		Abstain	N/A
4	LaGen	Richard Comeaux		Negative	Comments Submitted
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		None	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	Comments Submitted
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	Comments Submitted
4	South Mississippi Electric Power Association	Steve McElhaney		None	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Abstain	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Abstain	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Abstain	N/A
5	AEP	Thomas Foltz		Negative	Comments Submitted
5	Ameren - Ameren Missouri	Sam Dwyer		Abstain	N/A
5	APS - Arizona Public Service Co.	Stephanie Little		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Abstain	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		None	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		None	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	Comments Submitted
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Abstain	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Affirmative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		Affirmative	N/A
5	Kissimmee Utility Authority	Mike Blough		None	N/A
5	Lakeland Electric	Jim Howard		Negative	Comments Submitted
5	Lincoln Electric System	Kayleigh Wilkerson		Abstain	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		None	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		None	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Abstain	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Mike Avesing		Affirmative	N/A
5	National Grid USA	Elizabeth Spivak		Abstain	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Abstain	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	Comments Submitted
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		None	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Abstain	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Abstain	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		None	N/A
5	Seattle City Light	Mike Haynes		Negative	Comments Submitted
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	None	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		None	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Abstain	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	Comments Submitted
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Negative	Comments Submitted
6	Ameren - Ameren Services	Robert Quinlivan		Abstain	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Abstain	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		None	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Abstain	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Affirmative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Affirmative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		None	N/A
6	Los Angeles Department of Water and Power	Anton Vu		None	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Abstain	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Affirmative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Abstain	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		None	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Abstain	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		None	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Abstain	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Negative	Comments Submitted
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Abstain	N/A
6	Seattle City Light	Charles Freeman		Negative	Comments Submitted
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	Comments Submitted

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Abstain	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
7	Exxon Mobil	Jay Barnett		Affirmative	N/A
7	Luminant Mining Company LLC	Stewart Rake		Abstain	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Affirmative	N/A
8	David Kiguel	David Kiguel		Affirmative	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		Affirmative	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 351 of 351 entries

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-03 Cyber Security Supply Chain Risk Management CIP-005-6, CIP-010-3 and CIP-013-1

Formal Comment Period Open through June 15, 2017
Ballot Pools Open for Additional Members through May 31, 2017

Now Available

A 45-day formal comment period will be open through **8 p.m. Eastern, Thursday, June 15, 2017** for the following standards:

1. **CIP-005-6 - Cyber Security – Electronic Security Perimeter(s);**
2. **CIP-010-3 – Cyber Security — Configuration Change Management and Vulnerability Assessments;** and
3. **CIP-013-1 – Cyber Security – Supply Chain Risk Management**.

The standard drafting team's considerations of the responses received from the last comment period are reflected in the proposed standards.

Commenting

Use the electronic form to submit comments on the standard. If you experience any difficulties using the electronic form, contact Nasheema Santos An unofficial Word version of the comment form is posted on the project page.

Ballot Pools

The existing CIP-013-1 ballot pool was used for all of the ballots associated with this project. The ballot pools for CIP-005-6 and CIP-010-3 have been opened to allow stakeholders to join if they are not existing members. The ballot pools are open through **8 p.m. Eastern, Wednesday, May 31, 2017.** Registered Ballot Body members may join the ballot pools here.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

Initial ballots for CIP-005-6 and CIP-010-3, an additional ballot for CIP-013-1 as well as the non-binding polls of the associated Violation Risk Factors and Violation Severity Levels will be conducted **June 6-15, 2017**.

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

For more information or assistance, contact Senior Standards Developer, Mark Olson (via email), or at (404) 446-9760.

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

Comment Report

Project Name:	2016-03 Cyber Security Supply Chain Risk Management | CIP-005-6, CIP-010-3, CIP-013-1
Comment Period Start Date:	5/2/2017
Comment Period End Date:	6/15/2017
Associated Ballots:	2016-03 Cyber Security Supply Chain Risk Management CIP-005-6 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-010-3 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 AB 2 ST

There were 101 sets of responses, including comments from approximately 220 different people from approximately 141 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

9. Provide any additional comments for the SDT to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4,5,6	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE

					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
SRC	David Francis	1,2	FRCC,MRO,NPCC,RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC

					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
Associated Electric Cooperative, Inc.	Mark Riley	1		AECI & Member G&Ts	Mark Riley	Associated Electric Cooperative, Inc.	1	SERC
					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC
					Todd Bennett	Associated Electric Cooperative, Inc.	3	SERC
					Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC

					Stephen Pogue	M and A Electric Power Cooperative	3	SERC
					William Price	M and A Electric Power Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
Lower Colorado River Authority	Michael Shaw	6		LCRA Compliance	Teresa Cantwell	LCRA	1	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
BC Hydro and Power Authority	Patricia Robertson	1		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC

Randy MacDonald	New Brunswick Power	2	NPCC
Wayne Sipperly	New York Power Authority	4	NPCC
Glen Smith	Entergy Services	4	NPCC
Brian Robinson	Utility Services	5	NPCC
Bruce Metruck	New York Power Authority	6	NPCC
Alan Adamson	New York State Reliability Council	7	NPCC
Edward Bedder	Orange & Rockland Utilities	1	NPCC
David Burke	Orange & Rockland Utilities	3	NPCC
Michele Tondalo	UI	1	NPCC
Sylvain Clermont	Hydro Quebec	1	NPCC
Si Truc Phan	Hydro Quebec	2	NPCC
Helen Lainis	IESO	2	NPCC
Laura Mcleod	NB Power	1	NPCC
Michael Forte	Con Edison	1	NPCC
Kelly Silver	Con Edison	3	NPCC
Peter Yost	Con Edison	4	NPCC
Brian O'Boyle	Con Edison	5	NPCC
Michael Schiavone	National Grid	1	NPCC
Michael Jones	National Grid	3	NPCC
David Ramkalawan	Ontario Power Generation Inc.	5	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Kathleen Goodman	ISO-NE	2	NPCC
Greg Campoli	NYISO	2	NPCC
Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC

Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC
					David Weekley	MEAG Power	1	SERC
					Steven Grego	MEAG Power	5	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable
	Shannon Mickens	2	SPP RE		Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE

Southwest Power Pool, Inc. (RTO)				SPP Standards Review Group	Deborah McEndafffer	Midwest Energy, Inc	NA - Not Applicable	NA - Not Applicable
					Robert Gray	Board of Public Utilities (BPU) Kansas City, Kansas	3	SPP RE
					Louis Guidry	Cleco	1,3,5,6	SPP RE
					Megan Wagner	Westar Energy	6	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Charlie Freibert	LG&E and KU Energy, LLC	3	SERC
					Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Dan Wilson	LG&E and KU Energy, LLC	5	SERC
					Linn Oelker	LG&E and KU Energy, LLC	6	SERC
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Brazos Electric Power Cooperative, Inc.	BRAZOS	1,5	Texas RE

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.

Likes 0	
Dislikes 0	

Response

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

Recommend removing those items covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy

Likes 0	

Dislikes 0	

Response

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski

Answer	No
Document Name	

Comment

GRE supports the NRECA comments.

In R1, NRECA recommends that the SDT reiterate “high and medium impact” each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to “products or services provided to the Responsible Entity,” but 1.2.4 is not. We recommend adding this phrase to 1.2.4: “Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity.”

Further, we recommend further clarification to the term “vendor.” We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term “vendor” is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term “system integrators” is not well understood and request further clarification.

Likes 0	
Dislikes 0	

Response

Timothy Reyher - Eversource Energy - 5

Answer	No
Document Name	

Comment

Comments:

Concerned that the R1 guidance provides details which are beyond the scope of R1

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Recommend removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

{C}1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

-

- R1.2.2: “Coordination of responses to vendor-identified incidents….”, it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE notes that the proposed standard is not responsive to the FERC directive. FERC Order No. 829 P. 59 specifically states "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." The Note in Requirement R2, however, states: "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." Texas RE agrees that it is unreasonable to hold a registered entity accountable for a vendor's adherence to (or lack of adherence to) a contract. Texas RE agrees as the standard drafting team (SDT) claims obtaining specific controls in the negotiated contract may not be feasible at all times but Texas RE believes this is *best practice*. In fact, in most cases contracts for these types of systems typically include security provisions and set similar expectations as described in the standard. The proposed standards would prohibit the compliance monitor from verifying the registered entity implemented part 1.1 and sub-parts 1.2.1 through 1.2.7. Moreover, this verification is to ensure that the registered entities' plans are consistent with the contract's expectations and obligations of the parties.

Admittedly, there will be circumstances in which a contracts may not be consistent or silent as it pertains to the responsible entity's security management plans (e.g. existing contacts or contracts in which the responsible entity was unable to negotiate the appropriate terms into the contract.) In those circumstances, other evidence should be provided demonstrating that the responsible entity has processes to ensure the vendor is expected/obligated to act consistently with the responsible entity's cyber security risk management plans as it relates to the vendor's products or services. Therefore, the contracts should remain in scope as to demonstrate the mapping of expectations from the plan to the contract as far as vendor interactions for those specific items included in the standard and to advance best practices leading to a more reliable BES.

Additionally, Texas RE has the following concerns:

- In the current CIP-013-1 version, the SDT elected to restrict the scope of the Supply Chain process to Medium and High Impact Bulk Electric System (BES) Cyber Systems, as well as exclude Physical Access Controls (PACS), Electronic Access Control and Monitoring Systems (EACMS), and Protected Cyber Assets (PCAs) from the scope of the Standard. In doing so, the SDT appeared to rely on a number of commenters that suggested that FERC Order No. 829, P. 59 excluded these types of devices. Specifically, these commenters pointed to the following language in the FERC Order: "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." FERC Order No. 829, P. 59. Accordingly, it appears that the SDT has concluded that PACS, EACMS, and PCAs collectively do not fall within the scope of "industrial control system hardware" or "computing and networking services associated with bulk electric system operations."

Texas RE is concerned PACS, EACMS, and PCAs *do* fall within the scope of "industrial control system hardware" and "computing and networking services associated with bulk electric system operations" as those terms are used in FERC Order No. 829. PACS, EACMS, and PCAs are foundational equipment within a network's architecture. Moreover, these devices are vendor supported and exposed to the precise vulnerabilities identified in FERC's supply chain directive. Given these facts, Texas RE does not believe there is either a basis in FERC Order No. 829 or, more importantly, a reliability-based rationale for excluding them from the scope of CIP-013-1.

- Page 7, Part 1.1: While FERC Order No. 829 specifically uses the term “hardware”, Texas RE notes the word “hardware” is not used in the standard language. Texas RE recommends replacing the word equipment with the term hardware in order to be consistent with the FERC Order.

- Page 8, Section 1.2.6: Texas RE recommends the SDT define or provide examples of the term “*system-to-system remote access*” as this is a broad term which can be interpreted in many different ways.

Likes 0	
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts

Answer	No
Document Name	

Comment

AECI supports NRECA's comments provided below:

In R1, NRECA recommends that the SDT reiterate “high and medium impact” each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to “products or services provided to the Responsible Entity,” but 1.2.4 is not. We recommend adding this phrase to 1.2.4: “Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity.”

Further, we recommend further clarification to the term “vendor.” We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term “vendor” is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term “system integrators” is not well understood and request further clarification.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment

GTC supports NRECA comments:

In R1, NRECA recommends that the SDT reiterate “high and medium impact” each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to “products or services provided to the Responsible Entity,” but 1.2.4 is not. We recommend adding this phrase to 1.2.4: “Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity.”

Further, we recommend further clarification to the term “vendor.” We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term “vendor” is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term “system integrators” is not well understood and request further clarification.

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx

Comment

The following comment covers several of the questions in one comment, submitted by the Foundation for Resilient Societies, Nashua, NH.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments of the IRC with the exception of the comment on Requirement R1, Part 1.1.

Likes 0	

Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	

Comment

Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD’s reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

(“new” meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term “elements” be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	

Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	

Comment

Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD’s reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

(“new” meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term “elements” be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	

Dislikes 0	
Response	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD’s reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

(“new” meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term “elements” be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

In the Response to Comments the SDT asserts “Identifying and assessing cyber security risks in BES Cyber System planning. The SDT revised CIP-013-1 Requirement R1 Part 1.1 to “specify risks that Responsible Entities shall consider in planning for procurement of BES Cyber Systems“. Previously, commenters indicated that “the scope of cyber security risks being addressed in R1 is unclear**”**. The SDT removed unnecessary and unclear wording from Requirement R1s main requirement and revised Requirement R1 Part 1.1 to clarify the supply chain cyber security risks that must be addressed by the Responsible Entity in planning for the procurement of BES Cyber Systems.”

This change does not clearly identify the risks as previously noted by commenters.

Dominion recommends the following language change for CIP-013-1, R1 Part 1.1:

“Include one or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess, if applicable, the cyber security risk(s) of (i) procuring and installing vendor equipment and software; (ii) network architecture security; and (iii) transitions between vendor”

Dominion also recommends the following proposed language change for CIP-013-1 R1 Part 1.2:

“One or more process(es) used during procurement of BES Cyber Systems that address the following, as applicable:”

R3 needs to contain the caveat found in R2 that “[Revision] of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders).”

Likes 0	
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

Comments: Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD’s reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

(“new” meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term “elements” be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	
Response	

Shawn Abrams - Santee Cooper - 1	
Answer	No
Document Name	
Comment	

The intent and purpose of CIP-013 is very dependent upon the Implementation Guidance document. We appreciate the hard work of the SDT to provide this document to industry and it has valuable information. A concern is that auditors can only audit to the requirements within the standard so some of the comments are based on needing more clarification within the standard itself.

Language should be included in the standard (not just in the Rationale) that allows for inclusion of a clause in a procurement agreement stating that CIP-013 compliance must be met by the supplier unless it is either not offered or would significantly increase the cost of the agreement. (See CIP-013-1, Section B, Rationale for Requirement R1). This language in a procurement agreement, along with the supplier's stipulation that this compliance is either unavailable or will increase costs should constitute proof that CIP-013 compliance was considered by the Registered Entity but waived due to the supplier's inability to accommodate the requirement in a reasonable manner.

The standard should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a supply chain cyber security risk management plan or plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Santee Cooper is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

This standard will create the need for entities to have an inventory tracking mechanism of products that are purchased under the supply chain risk management plan. For example, switches could be purchased for use in an IT department, not under the supply chain cyber security risk management plan, and this would preclude it from being used in a BES Cyber System. A CIP Exceptional circumstance or something similar should be added to the standard to allow an entity to use a piece of equipment not procured under the supply chain cyber security risk management plan rather than risk reliability of the BES.

Please add some wording to the requirement in the standard to address how far up the supply chain the plan applies to. If a laptop is purchased from a vendor is there an expectation that the cyber security risk management plan stop with that vendor or is there an expectation that the associated parts of the laptop fall under the plan? It's currently included in the rationale language but the rationale language cannot be audited.

What happens when a vendor is bought out by another vendor? Are you compliant until you have to negotiate a contract with the new vendor?

In R1 Parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing "identified to "acknowledged" or "confirmed."

Likes 0	
Dislikes 0	
Response	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment
Recommend modifying CIP-007 and CIP-010 to include the proposed risk management elements proposed in CIP-013, or take the corresponding elements out of CIP-007 and CIP-010 to make CIP-013 more than just having a plan. There are no quantifiable measures in CIP-013 that really justify it as a stand-alone standard.

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment
Even though ReliabilityFirst believes the CIP-013-1 draft standard address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 and is a positive step in addressing cyber supply chain management, ReliabilityFirst Abstains mainly due to Requirement R1 missing Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following specific comments for consideration. 1. Requirement R1 i. Even though Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) were not specifically called out specifically in FERC Order 829, ReliabilityFirst believes the SDT needs to examine the possible risk of not including EACMS, PACS and PCA as part of Requirement R1 and go beyond what was stated in FERC Order 829. EACMs and PACS are critical cyber assets that control access and monitoring into the entities' ESPs and PSPs and should follow the Supply Chain standard/requirements as do the High and Medium Impact Cyber Systems. As for the PCAs, if they are compromised due to a vulnerability in the vendors supplied hardware or software, they can possibly affect high and medium impact BES Cyber Systems. ReliabilityFirst offers the following modifications for consideration: a. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber System and, [if applicable, associated Electronic Access Control and Monitoring (EACM), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA)]. The plan(s) shall include:

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	

Comment

- BC Hydro appreciates the direction of the revisions ie to remove enforcement actions against responsible entities that have limited ability to influence vendors. However, BC Hydro still believes some aspects of R1 will be difficult to manage / enforce, especially given the breadth of vendors many responsible entities have associated with their BCAs. Not all vendors are going to be able to accommodate the asks of the requirement.

- "Notification by the vendor…" suggests the vendor is expected to reach out to the responsible entity, and communication / transparency is endorsed through potential inclusion of terms in RFP's / contracts. This relies on the vendor honesty / transparency and there is no way to verify their attestations. The requirement focuses on entities reviewing vendor processes which may have limited impact on reliability.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

R1 states that each RE must have a plan with one or more processes that address ....as applicable. Applicability is in the eye-of-beholder, however the requirement does not specifically say as identified by the Responsibility Entity, which auditors may take as a deliberate act not to include, interpreting that it is not up to the Responsibilty Entity to determin which are applicable.

Likes 0	
Dislikes 0	

Response

Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5

Answer	No
Document Name	

Comment

The clarification that we don't have and would like from NERC/WECC is the intent of the following statement in CIP-013 R1.2.5 ***"Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System".*** There is no Guidelines and technical basis at the end of the standard for this

This has a very large implication as this says all software provided by a vendor has to perform an integrity and authenticity verification.

This could implicate a dedicated channel from the vendor validating through software certificates which would imply entities forcing software vendors to provide this mechanism, which the likelihood of meeting this for MS, Symantec, (non-control system software) is slim. MD5 checksums can not validate the integrity of the software as this hashing mechanism was broken in 2005 (although a lot of software vendors still use it).

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No
Document Name	

Comment

Reclamation recommends the proposed standard differentiate between contractual and non-contractual purchases, such as commercial off-the-shelf (COTS) products or other purchases made without using a contract vehicle (e.g., credit card purchases or using repurposed equipment).

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

Requirement R1.

Oncor agrees with the concept; however, Oncor believes the language for R1.1 should be revised as follows, *"(i) Responsible Entity procures and installs vendor equipment and software"*; and *"(ii) Responsible Entity transitions from one vendor(s) product or service to another vendor(s) product or service".*

For Requirement 1.2.1., the current wording suggests that the vendor has sufficient knowledge of Oncor's environment to know that a particular vulnerability does in fact pose a security risk to Oncor. We offer a recommendation on the language, *"Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that could pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.2. The current phrase "coordination of response" is not clear as to what is intended by "coordination". We offer a recommendation on the language, *"Coordination of response activities by the vendor and the Responsible Entity to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.3. The current wording suggests that the vendor has sufficient knowledge of Oncor to determine whether or not an individual should no longer be granted access. Oncor is the only party to an agreement that has the ability to determine who should or should not have access. We offer a recommendation on the language, *"Circumstances where vendors should notify the Responsible Entity that access requirements of the vendor or third party personnel has changed, based on CIP-004, R5."*

Requirement 1.2.4. The current wording is not clear as to which vulnerabilities are applicable. We offer a recommendation on the language, *"Disclosure by vendors of known vulnerabilities in the procured product or service that follows a responsible disclosure process";* Guidance should also be added to reference US-CERT, NIST, or other industry sources.

Requirement 1.2.6. Oncor suggests the following wording change as the use of the phrase "Coordination of controls" is confusing. We offer a recommendation on the language, *"Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)."*

Likes 0	
Dislikes 0	

Response

Andrew Meyers - Bonneville Power Administration - 6

Answer	No
Document Name	

Comment

BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	No

Document Name	

Comment

In R1, NRECA recommends that the SDT reiterate “high and medium impact” each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to “products or services provided to the Responsible Entity,” but 1.2.4 is not. We recommend adding this phrase to 1.2.4: “Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity.”

Further, we recommend further clarification to the term “vendor.” We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term “vendor” is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term “system integrators” is not well understood and request further clarification.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

Requirements R1 and R2 essentially shift the burden for ensuring that BES Cyber System hardware and software vendors, resellers, and integrators follow sound security management practices onto individual Responsible Entities, which N&ST considers both unfair and unreasonable, for small entities in particular. The just-endorsed (by NERC) CIP-013 Implementation Guidance document suggests an entity could address R1.1’s requirement to “identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services” by means of a series of interactions with prospective vendors that comprise, for all intents and purposes, a risk assessment of the vendor, conducted by the entity. What recourse would a small entity have if a prospective supplier, perhaps the only one available, declined to cooperate with such an in-depth examination of its internal processes? R2, which requires the implementation of the entity’s R1 plan(s), acknowledges a vendor may be disinclined to agree to contractual obligations to support one or more specific elements of an entity’s R1 risk management plan. However, it contains no language that acknowledges this could make it difficult, if not impossible, for the entity to fully implement its R1 plan. N&ST believes this creates significant compliance risks for entities that may have few if any other options in some procurement situations. N&ST therefore recommends the addition of language similar to existing technical feasibility language in CIP-002 through CIP-011.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.3 (revocation of vendor remote access privileges) in its CIP-004 Access Management and/or Access Revocation documentation.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.6 (vendor remote access) in its CIP-005 ESP and Interactive Remote Access documentation.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.5 (vendor software authenticity and integrity) in its CIP-010 Configuration Change Management documentation.

Initial CIP Senior Manager or delegate approval of risk management plan(s) should be added to R1. N&ST notes the initial implementation of R3 specified in the draft Implementation Plan is on or before the Effective Date. If that language is retained, there will be no need to add CIP Sr Manager or delegate approval to R1.

CIP-013 R2 and/or the Implementation Plan should contain “trigger” language for R2 that clarifies an entity must implement its R1 risk management plan(s) for new procurement contracts signed on or after the Effective Date of CIP-013. Entities with no new procurement contracts or no new in-progress procurements on the Effective Date should not be expected to be able to demonstrate compliance with R2 at that time.

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

NPPD supports the comments submitted by the MRO NSRF for CIP-013. In addition:

NPPD is concerned that this Standard is not sufficiently represented to be auditable. First, the Standard is not performance based, which leads to auditor discretion, which leads to inconsistency among the Regional Entities across the NERC footprint. Second, the Implementation Guidance document has words that protect the entities from interpretation risk, however are not part of the Standard; which leaves the auditor to determine the intent of the drafting team. This is true in the rationale section for R1 which has wording which would minimize interpretation risk to entities, however are not reflected in the Standard. The Rationale states that the supplier must meet CIP-013 unless it is either not offered by the supplier or would significantly increase the cost of the agreement. This needs to be included in the Standard or as a footnote in the Standard. This would be very important to clarity in audit practices. In addition, the Standard should specifically state that as long as evidence demonstrates that all items expressly identified in R1 are contained in the “plan” and are implemented via R2 that entities shall not be out of compliance (there should be no findings for opinion on intent or security).

As with other recently produced CIP Standards, this Standard is being “rushed” to satisfy a FERC directive and without concise and clear wording, implementation considerations of all impacted parties, and the means for auditors to audit to a performance based Standard and understood audit practices. An extended comment/balloting period should be requested of NERC/FERC in order to produce an auditable Standard.

Other comments:

There are no parameters for Standard applicability. If a piece of equipment is purchased and the vendor and entity meet the Standard, do subsequent purchases of associated parts relative to the equipment or replacement parts of the equipment from other vendors need to also meet the Standard?

R1 Parts 1.2.1 and 1.2.2 “vendor-identified incident” is not clear. This needs to have clarity added in the Standard. In addition “identified” should be changed to “confirmed”.

CIP-013 R1 parts 1.2.5 and 1.2.6 are covered in CIP-005 and CIP-010. CIP-013 parts 1.2.5 and 1.2.6 should be removed to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

Likes 0	
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 4

Answer	No
Document Name	

Comment

GSOC supports NRECA's Comments of:

In R1, NRECA recommends that the SDT reiterate “high and medium impact” each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to “products or services provided to the Responsible Entity,” but 1.2.4 is not. We recommend adding this phrase to 1.2.4: “Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity.”

Further, we recommend further clarification to the term “vendor.” We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term “vendor” is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term “system integrators” is not well understood and request further clarification.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	No
Document Name	

Comment

Requirements 1.2 through 1.2.4. are extremely difficult to negotiate and implement with vendors, especially across such a diverse industry and diverse set of vendors. As written, the requirements make the vendor responsible for providing notifications to the Responsibility Entity. This puts the burden on the Responsible Entity to enforce these requirements through contractual obligations. The rationale states that "such contract enforcement is not subject to this Reliability Standard;" however, the performance of these requirements belongs solely to entities that are outside the jurisdiction of NERC and the Commission and can be held accountable only through contraction enforcement. As written, these specific reliability requirements put the Responsible Entities in a precarious position of acting as a surrogate regulator on a secondary industry.

If the intent is not to make the Responsible Entity accountable from a compliance stand point for the actions of vendors or other parties, the language should be written into the requirement wording. The clause in R2.2 states this exception, but does not then clarify what the Responsible Entity is obligated to do. The Responsible Entity is supposed to negotiate those terms, try to obtain that information, but if they can't then is it still not a violation? Will the auditors also look at it from this perspective?

Furthermore, the language of the R1.2 to R1.2.4 should be changed to meet the SDT's objectives while relying solely on the actions of the Responsible Entity and not those of any other party. However, if the intent is to include the items in R1.2 in the process for consideration of risk when selecting a vendor or product during the procurement process as the draft guidance seems to indicate, then those intentions should be explicit in the requirement language.

There is no issue with Requirement 3 requiring a periodic assessment of the supply chain cyber security risk management controls in order to update plans, etc. However, a recurring review by business unit stakeholders should be sufficient. The requirement to have the CIP Senior Manager or delegate approve the plan is simply a formality and is administrative in nature and provides no further security value.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	No
Document Name	

Comment

- Please provide clarification on what a "contract" is. For instance, is an annual software license a contract?
- Please provide feedback as to what Registered Entities should do if vendors refuse to the specifications within the CIP-013 requirements.
- Please provide further clarifications and expectations within Measure 2 to ensure entities are prepared for compliance oversight expectations.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No

Document Name	

Comment

SPP offers comments on the subrequirements of R1, as follows:

R1.1 – SPP recommends that subpart (i) be modified to accommodate the procurement “and/or” installation of vendor equipment “and/or” software and, further, requests clarification as to the intended meaning of the “transitions from one vendor(s) to another vendor(s)” concept within the context of subpart (ii).

1.2.1 – SPP recommends that “products or services” be modified to reference “products and/or services.”

1.2.2 – SPP requests clarification as to the “coordination” intended to be imposed, suggesting that the requirement may stand alone with any coordination component removed.

1.2.4 – SPP recommends that the 1.2.4 be modified to appropriately limit vendor disclosure of known vulnerabilities to the products and/or services provided to the Responsible Entity, consistent with 1.2.1. In addition, SPP notes that there is a lack of consistency between 1.2.1 and 1.2.4 with the use of the terms “vendor equipment” and “software” in 1.2.1, but uses the term “products” in subrequirement 1.2.4. SPP seeks clarification on whether the SDT intends “products” to be broader than equipment and software. SPP recommends that the SDT be consistent and use “vendor equipment” and “software” throughout, or provide additional clarification about the scope of the term “products.”

1.2.6- SPP requests clarification as to the “coordination” intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. SPP believes the “coordination of controls” may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, SPP is concerned that it is unclear what is required for “coordination,” as well as how such coordination would be evidenced at audit.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG offers comments on the sub requirements of R1, as follows:

R1.1 – NRG recommends that subpart (i) be modified to accommodate the procurement “and/or” installation of vendor equipment “and/or” software and, further, requests clarification as to the intended meaning of the “transitions from one vendor(s) to another vendor(s)” concept within the context of subpart (ii).

1.2.1 – NRG recommends that “products or services” be modified to reference “products and/or services.”

1.2.2 – NRG requests clarification as to the “coordination” intended to be imposed, suggesting that the requirement may stand alone with any coordination component removed.

1.2.4 – NRG recommends that the 1.2.4 be modified to appropriately limit vendor disclosure of known vulnerabilities to the products and/or services provided to the Responsible Entity, consistent with 1.2.1. In addition, NRG notes that there is a lack of consistency between 1.2.1 and 1.2.4 with the use of the terms “vendor equipment” and “software” in 1.2.1, but uses the term “products” in sub requirement 1.2.4. NRG seeks clarification on whether the SDT intends “products” to be broader than equipment and software. NRG recommends that the SDT be consistent and use “vendor equipment” and “software” throughout, or provide additional clarification about the scope of the term “products.”

1.2.6- NRG requests clarification as to the “coordination” intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. NRG believes the “coordination of controls” may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, NRG is concerned that it is unclear what is required for “coordination,” as well as how such coordination would be evidenced at audit.

Additionally: NRG is concerned that the R1 guidance provides details which are beyond the scope of R1.

NRG requests that the NERC SDT consider re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. The Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

NRG recommends removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) that are covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear that there is a remaining need for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions

into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

NRG requests SDT consideration that: The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, NRG requests NERC SDT consideration of the assertion that Registered Entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

CIP-013-1 R1.2 – "One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: " The term "as applicable" implies it is optional. Who determines whether something is applicable or not? NRG suggests that NERC SDT remove it or provide additional clarity.

CIP-013-1 R1.2.3, NRG has concerns that it is not clear when vendors have to notify if remote or onsite access should no longer be granted to vendor representatives. 2 hrs, 24 hrs, or 3 months?

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

1.1 – Delete "planning for". Or if the use of "planning for" in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

-

- R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. NRG requests SDT consideration of suggestion to delete.

Furthermore, NRG requests NERC SDT consideration of the following comments:

· On page 6 of CIP-013 draft:

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

NRG requests that industry have the ability to accept a level of risk through internal risk assessment processes if a supplier is unwilling to negotiate and accept the cyber security terms into negotiated contracts.

· On page 6 of CIP-013 draft:

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

NRG requests that the term vendor be further clarified to specify if meaning developers, product resellers or system integrators of “third-party” software, system components, or information system services, etc (versus internal company developers).

· On page 8 of CIP-013 draft (under R2):

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

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.

NRG requests further understanding of what, if any expectations are to be included in T&Cs and what are the expectations of how the vendor will be expected to perform as the term “expectations” is listed on page 6 of the standard?

Likes 0	
Dislikes 0	

Response

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6

Answer	No
Document Name	

Comment

CIP-005 has had R2.4 and R2.5 added as they pertain to interactive user access and remote system to system access tracking. These were previously in the CIP-013 standard as part of the Supply Chain requirement. Due to CIP-005 R2 already dealing with an Intermediate system for Interactive Remote access, it seems logical that this requirement be expanded to include these.

The clarification that we don't have and would like from NERC/WECC is the intent of the following statement in CIP-013 R1.2.5 ***"Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System".*** There is no Guidelines and technical basis at the end of the standard for this

This has a very large implication as this says all software provided by a vendor has to perform an integrity and authenticity verification.

This could implicate a dedicated channel from the vendor validating through software certificates which would imply entities forcing software vendors to provide this mechanism, which the likelihood of meeting this for MS, Symantec, (non-control system software) is slim. MD5 checksums can not validate the integrity of the software as this hashing mechanism was broken in 2005 (although a lot of software vendors still use it).

So we need clarification on this before a vote recommendation can be established for CIP-013 R1.

Likes 0	
Dislikes 0	

Response

Mark Holman - PJM Interconnection, L.L.C. - 2

Answer	Yes
Document Name	

Comment

PJM agrees, with the following suggested edits:

Within 1.2.1 and 1.2.2, PJM feels that "incident" need further clarification as it is a bit broad (i.e. could be interpreted as anything from a phishing attempt to an actual breach). PJM suggests it be narrowed down to actual breaches. Additionally, "security risk to the Responsible Entity" should be "security risk to the BES." Lastly, we like how the notification and coordination pieces are split out.

Within 1.2.3, PJM suggests changing "no longer be granted" to "should be revoked" to strengthen the language.

Within 1.2.5, PJM suggests adding in “firmware” and “where the method to do so is available” as to match the CIP-010 language.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

The understanding of the intent and purpose of CIP-013 is very dependent on the Implementation Guidance document. There is no guarantee that this document will be approved by NERC even if CIP-013 is approved.

Request clarification on whether the SDT intends “products” to be broader than equipment and software. Recommend that the SDT be consistent and use “vendor equipment” and “software” throughout, or provide additional clarification about the scope of the term “products.”

There are concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, we recommend that all references to “contracts” and most references to “procurement” be struck from CIP-013, except the note in R2 that states:

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.

Our reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such we ask that R1.2 be revised as follows:

1.2. *One or more process(es) used in procuring for its newly procured BES Cyber Systems that address the following elements, as applicable:*

(“new” meaning obtained after the implementation of CIP-013).

Request that the term “elements” be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits or subtext in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately, there should be no expectation that such protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

In the absence of such a change, we requests substantial additional clarification about how, without contract terms and contract negotiations being auditable, performance of R2 implementation will be audited and assessed.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	

Comment

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.

Recommend removing CIP-013 R1 subparts 1.2.5 and 1.2.6 from CIP-013 since these are covered in CIP-005 and CIP-010. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

{C}1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

- R1.2.2: “Coordination of responses to vendor-identified incidents….”, it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.

Likes 0	

Dislikes 0	

Response

Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	

Comment

AZPS agrees with the proposed requirements in CIP-013-1 subject to the below requests for clarification and recommended revisions/additions.

· AZPS requests that the SDT consider and provide guidance regarding the applicability of the requirements of CIP-013-1 where the traditional procurement process is not applicable to a particular purchase. For example, software that is purchased from a retail source rather than a vendor is often purchased subject to existing retail terms and conditions and without the opportunity to negotiate additional terms and conditions around the procurement.

· AZPS further recommends the following changes/additions:

· Requirement 1.2.4 - "Disclosure by vendors of known vulnerabilities ***when they become known to the vendor.***"

· Requirement 1.2.5 as written is duplicative with CIP-010; hence, AZPS recommends this Requirement be deleted or revised to address the process for software integrity and authenticity, rather than actual verification of those.

· Requirement 1.2.6 – AZPS recommends removal of the word "coordination" and on the insertion of the term "identification" to address a process for identifying how a vendor handles controls.

· Requirement R2 – evidence may not be available for items that are purchased form a retail source, as noted above. AZPS recommends an exception be identified for this purpose.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	

Comment

Modify R1.2.5 as follows: "Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System when technically feasible; and". This will help address concerns with vendors such as Microsoft that pushes patches when they identify a need.

Add language to address allowable exception in the event of CIP Exceptional Circumstances for R2 (e.g. patches issued with ransomware attack in-progress needed immediate action to be taken).

Luminant would prefer that the CIP-013 standard be formatted similar to other CIP standards with the use of tables (e.g.CIP-004-6 Table R1).	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG request clarification, regarding R1.2.4, of whom the vulnerability must be known by to require disclosure and that it only be for the vendor's own products and only those supplied to the Responsible Entity. As stands, it might be interpreted that vulnerabilities might not need to be disclosed until publicly known, for products the Responsible Entity doesn't have, or for vulnerabilities the vendor might know in products other than its own. Suggest changing to "Disclosure by the vendor of vulnerabilities known to the vendor concerning products and services supplied by the vendor to the Responsible entity. Requirement R1 Part 1.2.4 requires additional clarification for the type of "known vulnerabilities" Vendor definition is required to avoid ambiguity; does the term vendor apply for contract employees/augmented staff/outsourcers? Are the requirements R1-R3 enforceable in exceptional circumstances?	
Likes 0	
Dislikes 0	
Response	

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
ACES supports the requirements to reduce the risk of remote access management. Using the CIP Applicability Section reduces the previous confusion of what BES Cyber Assets are in scope.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Concerned that the R1 guidance provides details which are beyond the scope of R1 Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going? In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.” Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005. Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).	

Recommend removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

1.1 – Delete "planning for". Or if the use of "planning for" in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

-

R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.

Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

See below comments.

Likes 0	
Dislikes 0	

Response

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	

Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	

Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?	
Likes 0	
Dislikes 0	
Response	

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
The Registered Entity suggests consider revising Section 1.2.3 to clarify under what circumstances vendors would be expected to notify the Registered Entity that vendor remotes access should be revoked. Regarding Section 1.2.4, suggest revising to clarify what type of vulnerabilities would be included in this disclosure.	
Likes 0	
Dislikes 0	
Response	

Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
R1-R2 are clearly stated and provide for the development and implementation of the required CIP-013-1 cyber security plans. R3 sets a clear expectation for periodic reviews and approvals. From an auditor's perspective, requiring the first review and approval of the R1 plan on or before the effective date of CIP-013-1 (Implementation Plan, Initial Performance of Periodic Requirements section, p. 3) provides clear guidance to industry on implementation expectations.	
Likes 0	
Dislikes 0	
Response	

Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response	

Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Regarding the use of the term “vendor,” as described in the “Rationale for Requirement R1” section of CIP-013-1: the SDT may want to clarify that staff augmentation contractors are not considered to be “vendors” in the context of the standard.	
Likes 0	
Dislikes 0	
Response	

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	

What is the difference between 1.2.1 and 1.2.4?

Why is the scope of 1.2.2 limited to vendor-identified incidents? What if a third party identifies an incident?

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?
- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?
- R1.2.2: “Coordination of responses to vendor-identified incidents….”, it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.

Likes 0	
Dislikes 0	
Response	

Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	

With respect to the proposed Requirement 1 Part 1.2.1, compliance requires the vendor to be responsive to vendor-identified incidents. We can only be compliant if the vendor releases such information. We can’t be held responsible for a vendor that does not provide incident related information. This verbiage has to be deemed acceptable when developing the plan(s).

With respect to the proposed Requirement 1 Part 1.2.4, compliance requires the vendor to be responsive to disclosing vulnerabilities. We can only be compliant if the vendor releases such information. We can’t be held responsible for a vendor that does not disclose vulnerabilities. This verbiage has to be deemed acceptable when developing the plan(s).

With respect to the proposed Requirement 1 Part 1.2.5, compliance requires cooperation by the vendor to participate in such a program. We will give procurement preference to vendors willing to participate however we are still at relying on vendor cooperation. We can’t be held responsible for a

vendor that does not provide accurate verification of software integrity and authenticity. This verbiage has to be deemed acceptable when developing the plan(s).

Likes 0	
Dislikes 0	

Response

Allan Long - Memphis Light, Gas and Water Division - 1

Answer	Yes
Document Name	

Comment

We support the comments submitted by APPA, including the following recommendations:

Re-word R1, Parts 1.2.1 and 1.2.4 to better describe what is expected. The endorsed Guidance does not adequately distinguish between the two parts.

"Vendor" is not a NERC-defined term and contributes ambiguity.

Those items (CIP-013 R1, Parts 1.2.5 and 1.2.6) covered in CIP-005 adn CIP-010 should be removed from CIP-013 to avoid duplication.

The Compliance and/or Implementation Guidance should make clear that, when evidence demonstrates that all items expressly identified in CIP-013 R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance.

There is concern about language related to procurement contracts, specifically the use of master agreements, piggyback agreements, and evergreen agreements. All references to "contracts" and most references to 'procurement" should be struck from CIP-013, except the note in R2.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

: Platte River Power Authority (PRPA) continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

PRPA agrees with limiting the requirement to high and medium assets only.

R1: PRPA generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

PRPA recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: PRPA agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

R3: PRPA agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, PRPA proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

For Requirement R 1, Part 1.2.4, CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") recommends the following modification to help clarify the type of disclosed vulnerabilities:

"Disclosure by vendors of known security vulnerabilities involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System."

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill

Answer	Yes
Document Name	

Comment

Even though the second proposed version of this standard has been simplified, SDG&E believes compliance with CIP-013-1 is potentially difficult and costly to demonstrate compliance.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

SMUD agrees with limiting the requirement to high and medium assets only.

R1: SMUD generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a Technical Feasibility Exception (TFE) or Asset Capability Exception, should be included in the standard for these kinds of procurement activities. An additional consideration is to allow agreements between the vendor and entity that will not cause a financial impact, such as a letter of understanding, commitment to a plan of action or other agreement.

SMUD recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	Yes
Document Name	

Comment

Austin Energy (AE) supports efforts to ensure the security of the Bulk Electric System and appreciates the time and effort the SDT put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

AE agrees with limiting the requirement to high and medium assets.

R1: AE generally agrees with the proposed R1 but has concerns about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and "piggyback" agreements. NERC should include an exception, comparable to a CIP Exceptional Circumstance, for such procurement activities.

AE recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts which require entities to perform the underlying function and take those functions into account during the procurement process is needless duplication which does not increase security or reliability and could result in compliance “double jeopardy.”

R2: AE agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in R1.

R3: AE agrees a 15-month review period is appropriate to review the supply chain cyber security risk management plan in R1.

Additionally, AE proposes the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date, similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Concerned that the R1 guidance provides details which are beyond the scope of R1 Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005. Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s). Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. Request to merge R1 Part 1.2.1 and 1.2.2 for the notification and the coordination related to vendor-identified incidents. Request to merge R1 Part 1.2.3 and Part 1.2.6 for the notification and the coordination of controls when remote or on site access are required and granted for (i) vendor-initiated interactive remote access, and (ii) system-to-system remote access with a vendor(s). The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.	
Likes 0	
Dislikes 0	
Response	
Theresa Allard - Minnkota Power Cooperative Inc. - 1	
Answer	Yes
Document Name	

Comment
See MRO NSRF comments.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment
SRP continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013. SRP agrees with limiting the requirement to high and medium assets only. R1: SRP generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities. SRP recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.” R2: SRP agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1. R3: SRP agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1. Additionally, SRP proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	

Comment
Even though the second proposed version of this standard has been simplified, SDG&E believes compliance with CIP-013-1 is potentially difficult and costly to demonstrate compliance.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	

Comment
While in overall agreement with Requirements 1 through 3, ACEC does have the following concern: The R1 and R2 requirements in the draft split the development of one or more documented supply chain cyber security risk management plan(s) (R1) and the implementation of those supply chain cyber security risk management plan(s) specified in Requirement R1 (R2). By splitting these the potential for violations have been increased from one (1) to two (2) – one for each requirement. It is recommended that R1 and R2 be combined to reduce the potential of multiple violations for what should be a single Requirement. To illustrate, a majority of the Standards have their development of plans, processes, or procedures and implementation of those plans, processes, or procedures in the same requirement: CIP-002-5.1 R1; CIP-003-6 R2, R4; CIP-004-6 R1, R2, R3, R4, R5; CIP-005-5 R1, R2; CIP-006-6 R1, R2, R3; CIP-007-6 R1, R2, R3, R4, R5; CIP-010-2 R1, R2, R3, R4; CIP-011-2 R1, R2

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	

Comment
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	

Comment

During the CIP-013-1 webinar on Feb 2, the SDT indicated several times that it is not the intention of R1 to force vendors to perform actions so that entities can comply with the standard. R1.2.1, R1.2.2, R1.2.3, R1.2.4 would force vendors to develop internal processes to notify entities of any changes relating to the requirements which would force vendors to take independent action to notify entities of any changes. Also, during the procurement phase, why would vendors reveal potential security flaws in their product above and beyond normal security patch notifications while they are competing against other vendors for the entities business? Also, entities have processes in place already for other CIP requirements to fully prepare an asset for deployment into the ESP. We don't grab equipment off of the back of the delivery truck and deploy it into the ESP immediately so what is the point of knowing about security flaws in their products during procurement? Any security flaws are probably already addressed with patches that will be downloaded and installed when preparing the asset for deployment. Also, a vulnerability assessment has to be performed against the asset and CIP-007/CIP-005 security controls have to be checked prior to deployment. 1.2.1, 1.2.2, 1.2.4, 1.2.5 appear to be redundant with CIP-007 R2 security patch management. Is the SDT expecting vendors to provide information about security/design flaws above and beyond the normal security patch notifications? If so, what kind of information would that be?

1.2.5 is troublesome as well (and it seems to be a duplicate of CIP-010-3 R1.6). Entities typically use update or proxy servers to discover and identify applicable security patches. For example, some use Windows Update Server Services to identify patches and roll them out once testing and approvals are complete. Do we need to check the check sums of the identified patches or can we trust that the update servers are authenticating the software?

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	

Comment

There is a lack of consistency between R1 parts 1.2.1 and 1.2.4 with respect to the use of the terms. While part 1.2.1 uses the "vendor equipment" and "software," part 1.2.4 uses the term "products." The SDT should clarify if it intends "products" to be broader in scope than equipment and software. USI recommends that the SDT be consistent and use "vendor equipment" and "software" throughout, or provide additional clarification about the scope of the term "products."

In R1 parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. USI suggests changing "identified to "acknowledged" or "confirmed."

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

USI believes the SDT should provide guidance regarding the use of the term “vendor.” If “Vendor” is not defined by NERC, the Guidance should recommend that Entities include their definition of “vendor” in their plan(s).

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits or subtext in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately there should be no expectation that such protections be achieved solely through the procurement process. Consistent with performance-based standards the objective is achieving each protection, not in how it is achieved.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

MMWEC supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	Yes
Document Name	

Comment

ITC Holdings agrees with the proposed requirements, however, we believe the wording of CIP-013 leaves a lot of room for interpretation. We recommend being more prescriptive in the wording of CIP-013 as well as providing detailed guidance in the Technical Guidance document.

Additionally, ITC Holdings agrees with the below comment submitted by SPP regarding the use of “coordination”:

1.2.6- SPP requests clarification as to the “coordination” intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. SPP believes the “coordination of controls” may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, SPP is concerned that it is unclear what is required for “coordination,” as well as how such coordination would be evidenced at audit.	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	

Comment
Requirement R1. The IRC has no issues with the concept. We offer a recommendation on the language, “(i) Responsible Entity procures and installs vendor equipment and software; and (ii) Responsible Entity transitions from one vendor(s) product or service to another vendor(s) product or service”. Note: **ERCOT does not support the above comment.** Requirement 1.2.1. The current wording suggests that the vendor has sufficient knowledge of the Responsible Entities’ environment to know that a particular vulnerability does in fact pose a security risk to the Responsible Entity. We offer a recommendation on the language, *“Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that could pose cyber security risk to the Responsible Entity;”* Requirement 1.2.2. The current phrase “coordination of response” is not clear as to what is intended by “coordination”. We offer a recommendation on the language, *“Coordination of response activities by the vendor and the Responsible Entity to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;”* Requirement 1.2.4. The current wording is not clear as to which vulnerabilities are applicable. We offer a recommendation on the language, *“Disclosure by vendors of known vulnerabilities in the procured product or service following a responsible disclosure process”.”* Requirement 1.2.6. The use of the phrase “Coordination of controls” is confusing. We offer a recommendation on the language, *“Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).”*

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2	
Answer	
Document Name	

Comment
The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	

Comment

I would support the comments of Andrew Gallo Austin Energy for all questions.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power

Answer	
Document Name	

Comment

MEAG supports the answers and comments of Salt River Project.

Likes 0	
Dislikes 0	

Response

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments of the IRC and offers the following additional comments:

Regarding Part 2.4, ERCOT is concerned that the meaning of "determining" in the phrase "have one or more methods for determining active vendor remote access sessions" is unclear. If the SDT's intent is to require *identification* of instances of active vendor remote access, ERCOT suggests rewording to "have one or more methods of *identifying instances of* active vendor remote access (including Interactive Remote Access and system-to-system remote access)."

ERCOT also requests clarification on the meaning of "system-to-system remote access." Interpreted broadly, this requirement could mean all ingress/egress network connections to the security zone. Identifying each instance of connection could become extremely burdensome, without providing any meaningful reliability benefit.

ERCOT recommends that the meaning of system-to-system remote access be qualified as vendor remote access which can do harm to the BES Cyber System (BCS) and recommends the following language:

"Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access). This is limited to sessions which have the ability to harm the BCS."

If the SDT declines to adopt this language, the SDT should consider defining "system-to-system remote access" or further clarifying the meaning of this term in the "Guideline and Technical Basis" section or in the Implementation Guidance.

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	

Comment

See comments in attached file

Likes 0	

Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
It remains unclear to us as to what the phrase “system-to-system” is meant to include. Please define or provide examples of what would be considered vendor “system-to-system” remote access.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	
Comments: The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question. Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-013. Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s). Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5 Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests additional clarity pertaining to the use of the term “active” in Requirement 2 Parts 2.4 and 2.5. As written, it could be interpreted that an entity would be required to monitor the remote access sessions of a vendor in real-time. Was this the drafting team’s intent with this language? If the drafting team’s intent was that an entity only be able to identify which vendor’s have remote access, we suggest revising the standard to more closely reflect said intent. If it is the drafting team’s intent that an entity must monitor in real-time the remote access of a vendor, additional guidance as to acceptable methods to achieve compliance with this intent is necessary.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
NPPD supports the comments for the MRO NSRF for this question.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Suggest rewording 2.4 to read, “Have one or more methods for determining when vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) are active.” Alternative wording would be, “Have one or more methods for identifying active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).”	
Likes 0	
Dislikes 0	

Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends that CIP-005-6 Requirement R2 Part 2.4 Requirements be changed to state, “Have one or more methods for determining and logging active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).” Reclamation recommends that the first bullet in CIP-005-6 Requirement R2 Part 2.4 Measures be changed to state, “Methods for accessing logged and actively monitored information to determine active vendor remote access sessions;” Reclamation also recommends that CIP-005-6 R2.3 be changed to "Where technically feasible, require multi-factor authentication for all Interactive Remote Access sessions" to align with CIP-007 R5, dealing with authentication requirements to help with consistency within the standards.	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	
Comment	
CIP-005-6 R2 Part 2.4 as drafted does not identify the “direction” of how system-to-system remote access is initiated. Interactive Remote Access specifies that it originates “from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity’s Electronic Security Perimeters”. Without defining the system of origin or other defining controls, similar to the definition of Interactive Remote Access, any connection from a CIP Cyber Asset to a vendor system, even if one-way and simply for data acquisition/submission, could be interpreted as subject to this requirement. Additional clarification is requested. Additionally, the Supplemental Material for the requirement points to a separate document without an official link. It appears this document has not been updated in six (6) years, and mostly targets securing Interactive Remote Access. It is requested that updated relevant material be placed in the Standard’s Supplemental Material section, similar to other CIP standards, and that the Supplemental Material section also attempt to provide guidance on the securing of system-to-system remote access.	
Likes 0	
Dislikes 0	

Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
I fully support the concept of monitoring and being able to terminate all remote acccess sessions, however as written the additional requirements have no timing aspects associated with them, have no component for notification or alerting on active sessions, are atrifically limited to vendor access only, (lower case vendor) so may not include contractors, service providers, etc. Cannot support the requirement as written.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
With the deletion of the language in R2, it now appears that every Responsible Entity needs to have a documented process for Interactive Remote Access, even if the Responsible Entity does not allow it. Why did the team delete this exemption language from R2 as it seemed to lessen the burden for those entities that do not allow Interactive Remote Access?	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
R2 part 2.4 should read: Have one or more methods for determining when vendor Interactive Remote Access and/or vendor system-to-system remote access sessions are active.	

Part 2.5 should read: Have one or more methods to disable active vendor Interactive Remote Access and/or vendor system-to-system remote access sessions).

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

The inclusion of (including Interactive Remote Access and system-to-system remote access) is problematic as the NERC defined term of Interactive Remote Access (IRA) explicitly excludes system-to-system process communication. Additionally, IRA already includes the concept of vendors (see 3) below).

"User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications."

The SDT should consider removing this system-to-system exclusion from the IRA defined term and stating Part 2.4 as –

Have one or more methods for determining active vendor Interactive Remote Access sessions.

And Part 2.5 as –

Have one or more method(s) to disable active vendor Interactive Remote Access sessions.

(note: the addition of 'sessions' in this Part to be consistent with Part 2.4.)

Lastly, from an SCRM perspective, the SDT should consider at least including some indication of when vendor remote access could or should be disrupted, but that may be better addressed in the CIP-013-1 R1.2.2 and/or R1.2.6 processes of the SCRM plan(s).

Likes 0	
Dislikes 0	

Response

Richard Vine - California ISO - 2

Answer	Yes
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

Please clarify definition of system-system communications.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

There needs to be a clear explanation of “machine-to-machine” and “system-to-system” remote access in the Guidelines & Technical Basis to provide the necessary understanding and scoping of these concepts for industry.

For example – “Machine-to-machine” or “system-to-system” remote access would include a logical connection between a High or Medium Impact BES Cyber System or it’s associated PCAs into or out of the associated ESP with a vendor-maintained Cyber Asset, and that connection does not have an interactive user access capability.

Additionally, under the Measures of R2.4, the statement of examples needs to have “such as” following “(including Interactive Remote Access and system-to-system remote access), such as:” to make it clearer that the below bulleted items are options an entity may choose from, and to be consistent with the formatting of R2.5.

Likes 0	
Dislikes 0	

Response

David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	Yes
Document Name	

Comment

The IRC agree with the new CIP-005-6 Requirement R2 Parts 2.4 and 2.5 however we note there is no corresponding “Guidance and Technical Basis” or “Rationale”. We also suggest that guidance be drafted to help entities understand what is intended by the term “Vendor” in relation to parts 2.4 and 2.5.

Regarding Part 2.4, the IRC is concerned that the meaning of “determining” in the phrase “have one or more methods for determining active vendor remote access sessions” is unclear. If the SDT’s intent is to require *identification* of instances of active vendor remote access, the IRC suggests rewording to “have one or more methods of *identifying instances of* active vendor remote access (including Interactive Remote Access and system-to-system remote access).”

Likes 0	

Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	

Comment
GTC supports NRECA comments: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	

Comment
The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question. Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-013. Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s). Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5 Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	

Response

Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	

AECI supports NRECA's comments provided below:

NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Texas RE agrees with the proposed requirements and has the following comments.

- Question 2 above uses the term "*machine-to-machine vendor remote access*". CIP-013-1 and CIP-005-6 use the term ""system-to-system remote access". Since these are two different terms, Texas RE recommends these terms be defined or examples provided to increase clarity and to avoid multiple interpretations.
- Section 4.2.3.5 – The language, "*Each Responsible Entity shall implement develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems*." is redundant with the requirement language. Also, neither CIP-013-1 nor CIP-010-3 contain this language in the Exemptions section.
- Page 1 Section 4.1.2.2 and Page 2 Section 4.2.1.2: Texas RE noted the term "*Special Protection System"* was removed. Texas RE recommends removing this term in all CIP standards.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	

Comment

The requirement in CIP-005-5 6 Table R2.4 states that an entity must have one or more processes to determine active vendor session. We would recommend adding ‘Active and Passive’ to the requirement since the Measures point to passive initiation in having the vendor call or receive permission before their remote access is granted. Additional guidance on what is ‘Active’ and whether the monitoring session requires tracking the entire session or initiation of the session would provide more clarity to industry.

Likes 0	
Dislikes 0	

Response

David Ramkalawan - Ontario Power Generation Inc. - 5

Answer	Yes
Document Name	

Comment

OPG suggest the term “vendor” be defined to exclude outsourcers that manage most aspects of a BES Cyber System. Normally they are contractually obligated to act in the Responsible Entities interests and fulfill or accommodate all compliance requirements. As such, this is a much closer relationship than is typically associated with the term “vendor”. Because in many such cases they would be principle maintainer or operator of said systems would often not technically feasible to disable the outsourcer’s access, remote or otherwise.

Requirement 2.4 mentions ability to determine “sessions”, not just “access”. Requirement 2.5 is ambiguous on whether it requires the ability to disable “active sessions” as opposed to merely disabling “active accounts”. Suggest replacing “access” in R2.5 with either “sessions” or “accounts” depending on what was intended or otherwise elaborating.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski

Answer	Yes
Document Name	

Comment

GRE requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.

Likes 0	

Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the inclusion of Parts 2.4 and 2.5 within CIP-005-6 R2; however, requests the statement “active vendor remote access sessions” be changed to “active vendor remote connection.” A vendor may sustain an active remote connection for longer than an individual active remote access session. Thus, a revision to the language would clarify the intent of this requirement, which is to monitor any time a vendor is connecting to and accessing sensitive cyber assets remotely. Thus, AZPS encourages the SDT to consider this revision as it will better ensure that active remote connections by vendors are monitored and addressed.	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Recommend creating a CIP-005-6 and CIP-010-3 ‘Guidance document’ similar to the one for CIP-013-1.	

Request that the narrative for the term 'Vendor' that is in the CIP-005-6 R2 Rationale box be added to the already Endorsed Guidance document for CIP-013-1 and to the Guidance documents for CIP-005-6 if it is created.

Request that a narrative for the term 'System-to-System' be added to the already Endorsed Guidance document for CIP-013-1 and to the Guidance documents for CIP-005-6 if it is created.

Recommend removing CIP-013 R1 subparts 1.2.6 from CIP-013 since it is covered in the proposed CIP-005-6.

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

Request more guidance for the term “vendor” and use cases. If “Vendor” is not defined by NERC, the guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 0	
Dislikes 0	

Response

Mark Holman - PJM Interconnection, L.L.C. - 2

Answer	Yes
Document Name	

Comment

As currently written, it is ambiguous in 2.4 as to why an entity needs to "determine" vendor access, especially in conjunction with the logging, monitoring and control activities described within the measures. PJM suggests combining 2.4 and 2.5 together ("Have one or more method(s) to determine and disable active vendor remote access sessions…").

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	Yes
Document Name	

Comment

ITC Holdings agrees with the below comment submitted by MRO's NSRF:

The NSRF question the use of "…*active* vendor…" in part 2.4 and 2.5 Requirements. The word "active" could mean either "the vendor is currently allowed electronic access and is currently within a BES Cyber Asset" OR "the vendor is idle and but has electronic access to a BES Cyber Asset". The NSRF recommends that "active" be removed as this will provide clarity to applicable entities. If active sessions was the SDT thought process, please state that within the proposed part.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question.

The definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-013.

Request more guidance for the term "vendor" and use cases. Guidance should prompt Entities to include their definition of "vendor" in their plan(s).

Regarding CIP-005-6, R2.4 & R2.5; NRG requests that the NERC SDT define or further clarify the meaning of “system-to-system” remote access.

NRG asserts that Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Please include a reference to FERC Order 829 for Parts 2.4 and 2.5.

Please consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

MMWEC supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1

Answer	Yes
Document Name	

Comment

Does system to system remote access include “read-only” access or all forms of external access from vendors?

Likes 0	
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 4

Answer	Yes

Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
The proposed CIP-005-6 uses vendor. Definition of vendor is not a NERC defined term. USI believes the SDT should provide guidance regarding the use of the term “vendor.” If “Vendor” is not defined by NERC, the Guidance should recommend that Entities include their definition of “vendor” in their plan(s). The SDT should consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
As stated, this requirement seems to start with the base assumption that the Registered Entity allows vendors to have Remote Access to the Registered Entity’s BES Cyber Assets with External Routable Connectivity (ERC), and therefore must implement a method to detect active vendor remote access session and have a method for disabling vendor access. Many Registered Entities do not allow vendors to have Remote Access to substation medium BES Cyber Assets. Would this relieve such REs from having to then develop a method to detect and disable active vendor remote access session and would documentation demonstrating that Vendor Remote Access was not allowed be sufficient?	
Likes 0	
Dislikes 0	

Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	

Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

The definition of “vendor” is important for defining and carrying out its compliance objectives for the requirements parts 2.4 and 2.5. The drafting team should add a part of one or both requirements to include a specific definition of vendor to support the related compliance procedures and evidence required of an entity.

For Part 2.4, it is not clear if the requirement applies to contractors and service vendors that are provided authorized access under CIP-004. Additionally, more information is needed on the meaning of “active”. Most of this is captured in logs after the fact. Does the drafting team intend for “active” to imply real-time information? Please clarify if the requirement only applies to a connection from the vendor directly to a system within the ESP or does it apply to connections from a vendor to a system outside the ESP that updates one inside the ESP.

For Part 2.5, Oncor would like clarification of the action, or examples, for when access should be disabled.

Likes 0	
Dislikes 0	
Response	

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP agrees with R2 Part 2.4 but requests clarification of the term “determining.”

SRP generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “…is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. SRP requests changing the language to “upon detected unauthorized activity.”

Likes 0	
Dislikes 0	
Response	

Normande Bouffard - Hydro-Qu?bec Production - 5	
Answer	Yes

Document Name	

Comment

Request to defined the scope of the requirements “for new contracts only”

With no defined scope, if the standard become effective in same time of the standard CIP-013-1, no terms will existed beetween entities and vendor in effective contracts. How the entities will comply to requirements ?

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “active vendor remote access sessions” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment

See atttached comments.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	Yes
Document Name	

Comment

BC Hydro sees value in adding the machine to machine vendor remote access component.

Likes 0	

Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	

Comment
AE agrees with R2 Part 2.4 but requests clarification of the term “determining.” AE generally agrees with Proposed R2 Part 2.5, but requests revisions to the rationale for R2. The last sentence of paragraph 2 states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. AE requests changing the language to “upon detected unauthorized activity.”

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	

Comment
SMUD agrees with R2 Part 2.4 but requests clarification of the term “determining.” SMUD generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. SMUD requests changing the language to “upon detected unauthorized activity.” Clarification or formal definition of the term ‘vendor’ should be considered. ICCP and DNP3 traffic is routine system-to-system remote

access between utilities, Operation and Maintenance vendors and other partners to provide reliability, without the term ‘vendor’ clarified, these protocols may fall into scope unnecessarily.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

PRPA agrees with R2 Part 2.4 but requests clarification of the term “determining.”

PRPA generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. PRPA requests changing the language to “upon detected unauthorized activity.”

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10

Answer	Yes
Document Name	

Comment

ReliabilityFirst agrees the changes to CIP-005-6 address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 to develop a new or modified standard to address “supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.” ReliabilityFirst offers the following specific comments for consideration.

1. Requirement R2 Part 2.3
    i. To be consistent with Parts 2.1 and 2.2 in the Standard, ReliabilityFirst offers the following modifications for consideration:
        a. [For all Interactive Remote Access sessions, require] multi-factor authentication.
2. Requirement R2 Part 2.4

i. ReliabilityFirst believes more context should be placed around the term “determining”. ReliabilityFirst offers the following modifications for consideration:

a. Have one or more method(s) for [authorizing, monitoring, and logging] active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Likes 0	
Dislikes 0	

Response

Allan Long - Memphis Light, Gas and Water Division - 1

Answer	Yes
Document Name	

Comment

Because the term "vendor" is not a NERC-defined term, the SDT should provide guidance regarding its use.

A "CIP Exceptional Circumstance" clause should be added to R2, Parts 2.4 and 2.5.

Likes 0	
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5

Answer	Yes
Document Name	

Comment

A definition of “vendor” is necessary. This should be interpreted as any third-party that initiates a remote access session. Not every third-party is necessarily considered a “vendor” based on generally accepted definitions.

With respect to the proposed Requirement 2 Part 2.4, additional details need to be provided on the expectations of “determining active vendor remote access sessions”. Two of the proposed measures state, “Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; **or** Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.” The former will be difficult to actively monitor for remote access. Remote access can be monitored, but this activity is too resource intensive to monitor in real-time. If it is necessary to actively monitor remote access in real-time then additional guidance is necessary. The latter is easily implemented. It is uncertain whether this requirement is expecting constant monitoring during the remote access session or just controlling access and logging the access. A more detailed expectation on the use of the reference tools is necessary.

Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
As in Question 1, regarding the use of the term “vendor,” as described in the “Rationale for Requirement R2” section of CIP-005-6: the SDT may want to clarify that staff augmentation contractors are not considered to be “vendors” in the context of the standard.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	

Response
Mick Neshem - Public Utility District No. 1 of Chelan County - 3
Answer	Yes
Document Name	
Comment
CHPD supports these changes.
Likes 0	
Dislikes 0	
Response
Chad Bowman - Public Utility District No. 1 of Chelan County - 1
Answer	Yes
Document Name	
Comment
CHPD supports these changes.
Likes 0	
Dislikes 0	
Response
Haley Sousa - Public Utility District No. 1 of Chelan County - 5
Answer	Yes
Document Name	
Comment
CHPD supports these changes.
Likes 0	
Dislikes 0	
Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
We request clarification on whether “system-to-system” access applies to access that is “one-way” where the remote end conducts only monitoring activity and no control is possible, or whether the SDT intent is that any system-to-system access be included. We would suggest that the SDT add verbiage to the Guidelines and Technical Basis making the distinction for each type of “active vendor remote access sessions” that are included in this requirement (Interactive Remote Access, system-to-system remote access with control, and/or system-to-system remote access for monitoring only). Another suggestion would be to create a formal NERC definition of system-to-system access.	
Likes 0	
Dislikes 0	
Response	

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
Please clarify definition of system-system communications	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	

Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	
Document Name	
Comment	
The NSRF question the use of "…*active* vendor…" in part 2.4 and 2.5 Requirements. The word "active" could mean either "the vendor is currently allowed electronic access and is currently within a BES Cyber Asset" OR "the vendor is idle and but has electronic access to a BES Cyber Asset". The NSRF recommends that "active" be removed as this will provide clarity to applicable entities. If active sessions was the SDT thought process, please state that within the proposed part.	
Likes 0	
Dislikes 0	
Response	

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

Disagree with the revisions on CIP-010-3, would like to see guideline language of verifying once be moved to the requirement/measure

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	No
Document Name	

Comment

Need additional information regarding how to verify integrity of software.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy requests additional guidance as to what constitutes acceptable verification of integrity as required by R1.6.2. The measure indicates that a change request record could demonstrate that source identity and integrity verification took place, but doesn't go into further detail as to what an acceptable check into source identity and software would be. Is there specific language that should be stated in the change request record that would clearly state the verification took place? More guidance on this aspect is requested.

Also, Duke Energy requests that the Note under Applicable Systems in Part 1.6 should remain there once the standard is approved. The Note provides valuable details as to the true scope of the Requirement, and aids entities in knowing what will be the compliance expectation.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	
Comments: The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many VSL does not cover the failure to implement the process. Does not include all of the combinations. Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions: How does one prove that a method is not available? What is the line between available/unavailable? How far do you have to go? We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.	
Likes 0	

Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	

Comment

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions:

How does one prove that a method is not available?

What is the line between available/unavailable? How far do you have to go?

We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	

Response

David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	

Comment
The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection.

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	

Comment
See attached integrated comments.

Likes 0	
Dislikes 0	

Response

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	

Comment
To avoid an interpretation of this requirement that may be overly burdensome, ERCOT suggests the following clarifications to the language in the requirement and measure of CIP-010-3 R1 Part 1.6. This would ensure a more holistic and less prescriptive approach to changes that deviate from the baseline. In the first sentence of Requirement R1.6, revise “For a change that deviates” to “Where technically feasible, for changes that deviate…” Revise the R1.6 Measure to read “An example of evidence may include, but is not limited to, a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed during the baseline change*, or a process which documents the mechanisms in place that would automatically ensure the authenticity and integrity of the software.”*

Likes 0	

Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 “Note:” within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; “CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.” CIP-010 R1.6 – Applicable System Note *“Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.”*	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD believes the R1.6 “Note:” within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; “CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.”

CIP-010 R1.6 – Applicable System Note

“Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.”

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	

Comment

CHPD believes the R1.6 “Note:” within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; “CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.”

CIP-010 R1.6 – Applicable System Note

“Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.”

Likes 0	
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	No
Document Name	

Comment

CHPD believes the R1.6 “Note:” within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; “CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.”

CIP-010 R1.6 – Applicable System Note

“Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.”

Likes 0	
Dislikes 0	

Response

Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1

Answer	No
Document Name	

Comment

The language should make clear that verification is required for the software intake process, but not for each subsequent installation.

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions:

- How does one prove that a method is not available?
- What is the line between available/unavailable? How far do you have to go?

We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

Likes 0	
Dislikes 0	

Response

Shawn Abrams - Santee Cooper - 1

Answer	No
Document Name	

Comment

Need clarification about how the addition of R1.6 applies only to BES Cyber Systems that are newly implemented and thus did not previously have a baseline and as such do not have an existing baseline to deviate from. Please clarify that this is for new BES Cyber Systems to avoid confusion and challenges during an aduit.

Need some additional examples of what constitutes evidence to meet compliance to this standard. Some systems are not connected to the internet purposefully and as such patches are installed utilizing a CD/DVD provided by the vendor. What would constitute appropriate evidence for a case such as this?

This requirement is not clear whether an entity has to duplicate efforts for every case for which such verification has to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that an entity can verify once and apply to many assets.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5	
Answer	No
Document Name	

Comment

Since the intent of CIP-010-3 R1.6 is a proactive verification of software integrity, R1.6 should focus on a single verification prior to introducing vendor software into the production environment. The current language of R1.6 utilizes a retroactive focus via baseline deviations. Please see the suggested wording - “Prior to introducing software not resident in baseline items (per 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.”

Likes 0	
Dislikes 0	

Response

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	

Comment

Proposed Requirement R1 Part 1.6 appears to require verification of identity and integrity of applicable changes to the baseline. However, the measure for this requirement gives an example of having a process, e.g., a change request record, instead of a specific example of verification. Can the team clarify the measure for this Requirement as an entity can have a change ticket process that merely requires the user to click a button that states that the software has been verified, however, if the team believes proof of such check, such as a screenshot of the vendor site, is required, please state such as an example.

Additionally, the example of evidence does not demonstrate how a software source or the software integrity is verified. An internal change ticket is not a verification of the software source. If they are going to push for source verification then modify CIP-007 R2.1 to include it. Specifically, what is expected as evidence -- a hash, screenshot, attestation, digital signature?

Likes 0	
Dislikes 0	

Response

Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	

Comment

Even though ReliabilityFirst believes the changes to CIP-010-3 draft standard address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 and is a positive step in addressing cyber supply chain management, ReliabilityFirst Abstains mainly due to Requirement R1 missing Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following specific comments for consideration.

1. Requirement R1 Part 1.6
2.
    i. ReliabilityFirst believes the “Applicable Systems” under Requirement R1 Part 1.6 should be consistent with “Applicable Systems” under parts 1.1, since sub-parts (Part 1.1.1, 1.1.2, & 1.1.5) are called out under the “Requirements” section for Part 1.6. EACMs and PACS are critical cyber assets that control access and monitoring into the entities’ ESPs and PSPs and should follow the Supply Chain standard/requirements as do the High and Medium Impact Cyber Systems. As for the PCAs, if they are compromised due to a vulnerability in the vendors supplied hardware or software, they can possibly affect high and medium impact BES Cyber Systems. ReliabilityFirst offers the following modifications for consideration for the “Applicable Systems” column in Requirement R1 Part 1.6:
        a. High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA
        b. Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA

3. Requirement R1 Part 1.6.3 (new sub-part)

    i. ReliabilityFirst believes a new sub-part 1.6.3 should be added to address the verification of the baseline configuration. ReliabilityFirst offers the following new sub-part 1.6.3 for consideration:

        a. Verify the deviations from the baseline configuration.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro does not agree with value-add of this standard requirement. Under current CIP requirements, CIP controls around testing of changes and ongoing monitoring of systems would mitigate any risk associated with software identity or integrity.

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 5

Answer	No
Document Name	

Comment

Ther is nothing wrong with the concept of the requiment however the language of the requirement is not supportable. The term available could me technically available, procedurally available, contracturaly available, freely available (no support purchase required). As written this requirement by its nature will be implemented and assessed drastically differently by different Responsible Entities. One could argue that only if all the available methods listed above exist in unison is software actually available.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

There are auditing challenges around the phrase “when the method to do so is available to the Responsible Entity from the software source” as it is hard to prove a negative. Oncor believes that verification of software source and integrity can take many forms. To take into consideration legacy software, Oncor believes the wording should be adjusted, to reflect FERC intentions that the requirements are forward looking, by replacing the phrase *“and when the method to do so is available to the Responsible Entity from the software source”* with *“and, at a minimum, for the portion of the software that has changed:”*

Second, the proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). We offer a recommendation on the language, *“Document and implement a software source management process to address source identity verification and media integrity controls on the software repository used for changes that deviate from the existing baseline configuration associated with items in parts 1.1.1, 1.1.2, and 1.1.5.”*

This process must include steps:

• To verify the identity of the software source when the method to do so is available; and

• To verify the integrity of the software obtained when the method to do so is available.

Evidence may include verification of identity of the software source and integrity of the software was performed for repository updates.”

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

NPPD supports the comments of the MRO NSRF, in addition:

Auditors will have too much discretion as to what is or is not enough for a validation check of each vendor, which will lead to inconsistencies across the NERC RE footprint. It is up to entities to document what the vendor is willing to do and hope the auditors agree it is enough to continue doing business with the vendor. Also, the language of the requirement says “…when the method to do so is available…”. If a vendor does not have a method to do so, but does in the next year or so, the entity may have a possible violation if it did not realize there was a change in the vendor’s available methods. This would force entities to periodically check to see if the vendor capabilities have changed. What is the period that would not make this a violation? The requirement is very vague.

Likes 0	
Dislikes 0	

Response

Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	

As currently written, “verify the identity” is too vague. PJM suggests adding examples of “identify” into the measure. PJM also suggests removing the word “software” from 1.6.1 and 1.6.2 as it is already stated within parts 1.1.1, 1.1.2 and 1.1.5 (firmware should be within the scope of 1.6).

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence.

We support these changes, but requests clarification about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	

Request clarification on how an Entity can verify the ‘integrity and authenticity’ one time and then be able to install on multiple devices.

Recommend removing CIP-013 R1 subparts 1.2.5 from CIP-013 since it is covered in the proposed CIP-010-3

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions:

How does one prove that a method is not available?

What is the line between available/unavailable? How far do you have to go?

We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

Likes 0	
Dislikes 0	

Response

Stephanie Little - Stephanie Little

Answer	Yes
Document Name	

Comment

To ensure that resources are appropriately focused on changes to be applied, AZPS recommends clarifying that verification should be completed “prior to application of a change.” Such a clarification will signal to entities that verification only needs to be performed where a change will be applied and avoid circumstances where a change is being evaluated for application and verification occurs, but the change is not applied. Under the current obligation, it is likely that verifications and associated evidence would be prepared regardless of whether the change is or is not applied and would therefore result in the dedication of resources to efforts that would have no benefit to reliability or security.

Additionally, AZPS requests clarification regarding the continued need for verification evidence where such is not available from the vendor. Specifically, AZPS notes that, where a vendor’s policy does not provide the necessary evidence associated with verification, this Requirement may frequently represent null evidence for areas where items are reviewed each time a change occurs, but no data is available due to the vendor’s policies. Such efforts would be redundant and of little or no value to security and reliability.

Likes 0	
Dislikes 0	

Response

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Add language to address CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE and NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: “For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer.” This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG suggest that 1.6.1 state “Verify the software originated from the vendor’s official source(s)”. In the current text, even if a source has an “identity”, it should also state the “identity” is the one that is expected. Similarly we can change the word “identity” with “correct identity” in R1 Part 1.6.1.	
Likes 0	
Dislikes 0	
Response	

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
By adding the “when the method to do so is available to the Entity from the software source” does this require the entity to document and detail what method is available of not available? How does that entity prove and document this condition? Does the entity have to document and prove that it was tested and verified for software integrity and authenticity? If so, what are those requirements, documentation, testing environment required and timeline for testing the software?	
Likes 0	
Dislikes 0	
Response	

Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
AECI supports NRECA's comments provided below: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: “For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer.” This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	

Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	

Comment
GTC supports NRECA comments: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: “For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer.” This sentence seems to be incomplete and further words are needed to complete it.

Likes 0	
Dislikes 0	

Response

Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	

Comment
EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated: For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without **verification that the component has been digitally signed** to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides **examples of controls for addressing the Commission’s directive regarding this first objective. Other security controls also could meet this objective.** Order No 829 at P 50 (emphasis added). Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read (“Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and

authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.

Likes 0	
Dislikes 0	

Response

Pablo Onate - El Paso Electric Company - 1

Answer	Yes
Document Name	

Comment

EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated:

For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without **verification that the component has been digitally signed** to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides **examples of controls for addressing the Commission's directive regarding this first objective. Other security controls also could meet this objective.** Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.

Likes 0	
Dislikes 0	

Response

Rhonda Bryant - El Paso Electric Company - 3

Answer	Yes
Document Name	

Comment

EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated:

For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without verification that the component has been digitally signed to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing the Commission's directive regarding this first objective. Other security controls also could meet this objective. Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes

Document Name	
Comment	

Additional examples of acceptable evidence would be helpful under the Measures column of the requirement.

Change the statement in the Guidelines and Technical Basis, Section Software Integrity and Authenticity, paragraph 1, third sentence: “The intent of the SDT is to provide controls for verifying the baseline elements that are *updated* by vendors.” to say “… *provided* by vendors.”

Additional clarity is needed regarding the following in the Guidelines and Technical Basis: “It is not the intent of the SDT to require a verification of each source *or software update at the time it is obtained*. It is sufficient to *establish the reliable source and software update once*. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” This is confusing because saying “each source or software update” is not required to be validated at the time it is obtained could be interpreted to mean continuous patch updates provided by a single vendor are only required to be verified once for the lifetime of the supply of patches from that vendor.

Additional examples of acceptable methods and evidence are needed in the Guidelines and Technical Basis for performing software integrity and authenticity.

For example – Consider having the measures for R1.6 be similar to R1.1.

Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1

Answer	Yes
Document Name	
Comment	

Disagree with the revisions on CIP-010-3. We would like to see guideline language of verifying once be moved to the requirement/measure.

Likes 0	
Dislikes 0	
Response	

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.

Likes 0	
Dislikes 0	

Response

Franklin Lu - Snohomish County PUD No. 1 - 6

Answer	Yes
Document Name	

Comment

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

We request clarification on the timing of requirement 1.6; specifically, on whether 1.6 must be completed before being placed in operation on a BES Cyber System. This distinction was made in the previous draft ("one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems"). Under the current language, it appears sub-requirement 1.6 could be done before or after the software is placed on a BES Cyber System. We suggest the SDT add a timeframe similar to the other CIP-010 R1 sub-requirements. For example, 1.3 states "within 30 days" while 1.4.1 states "prior to the change". Additionally, we request adding 1.1.3 (any custom software installed) to 1.6, as custom software could be internally or externally provided, and needs to be verified for integrity and authenticity.

Likes 0	
Dislikes 0	

Response

Bob Thomas - Illinois Municipal Electric Agency - 4

Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
No issues from an SCRM perspective. Part 1.6 is generic and can be considered a good idea for all changes from baseline configurations described in Parts 1.1.1, 1.1.2, and 1.1.5.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	

Comment
Need to emphasize the phrase “and when the method to do so is available to the Responsible Entity for the software source”. Since this is a non-prescriptive requirement it is expected that we will be demonstrating compliance by implementing the plan(s) required in CIP-013. Since it may not be possible to hold the software resource directly responsible it is expected that the demonstration of “best effort” will be sufficient and not subject to interpretation by the Compliance Enforcement Authority. Recommend providing more examples of suitable evidence that should be gathered to verify identity and integrity. The Measure as currently written is too vague.

Likes 0	
Dislikes 0	

Response

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	

Comment
We support APPA's submitted comments, including: This requirement would possibly involve entitites duplicating effort for every case for which such verification had to be undertaken. More examples of evidence should be provided. Clarification is needed about how new R1.6 applies to entirely new BES Cyber Systems.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	

Comment

PRPA agrees this requirement belongs in CIP-010 R1. PRPA generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- PRPA recommends the Guidelines and Technical Basis section is updated to reflect current information.
    - The requirement states “For 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…,” indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”
    - PRPA also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.
- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, PRPA requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While PRPA supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

The Guidelines and Technical Basis of CIP-010-3 states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

CenterPoint Energy recommends incorporating this concept in the R2 requirement language in order to clarify that integrity and authenticity do not need to be verified for every source or software update, and that the download once and install on many approach is acceptable if the integrity and authenticity of the downloaded software are validated. CenterPoint Energy recommends adding the following language to Requirement R2:

Upon validation of the integrity and authenticity of software, a Responsible Entity does not need to verify the integrity and authenticity for subsequent updates of such software.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD agrees this requirement belongs in CIP-010 R1. SMUD generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- SMUD recommends the Guidelines and Technical Basis section is updated to reflect current information.
  -
    - The requirement states “For 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…,” indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”
    - SMUD also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.
  - There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in

order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.

- Additional examples of acceptable measures should to be listed. Additionally, SMUD requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.

- While SMUD supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

-

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	Yes
Document Name	

Comment

AE agrees this requirement belongs in CIP-010 R1 and generally agrees with Proposed R1 Part 1.6, but request the SDT address the following items:

AE recommends the Guidelines and Technical Basis section be updated to reflect current information.

The requirement states “For 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…,” indicating the authenticity and integrity of the specified parts must be verified each time a baseline changes for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to occur (e.g., in the cases of multiple installations of software across many applicable Cyber Assets). This requirement does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe the existing statement in the GTB provides clarity on this issue and request it not be removed. From the GTB: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

o AE also recommends rewording the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

o There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.

o Additional examples of acceptable measures should to be listed. Additionally, AE requests examples of acceptable evidence when there is no method available to verify the identity of the software source.

While AE supports these changes, clarification is required about how R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS newly implemented and which have no previous baseline, and thus do not have an existing baseline from which a change can occur. We expect R1.6 is intended to apply to new BCS as well as to existing BCS but, as written, the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment

See attached comments

Likes 0	
Dislikes 0	

Response

Normande Bouffard - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

Request to defined the scope of the requirements “for new contracts only”

With no defined scope, if the standard become effective in same time of the standard CIP-013-1, no terms will existed beetween entities and vendor for effective contracts. How the entities will be conformed to requirements ?

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection.

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees this requirement belongs in CIP-010 R1. SRP generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- SRP recommends the Guidelines and Technical Basis section is updated to reflect current information.
    - The requirement states “For 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…,” indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”
    - SRP also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.
- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, SRP requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While SRP supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We

expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: “For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer.” This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	

N&ST believes the “if you can, you must” qualifying language in this proposed requirement part should be added to at least some parts of CIP-013 R1 and R2.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	Yes
Document Name	

Comment

The NSRF has the same comment from CIP-013-1 R1: CIP-010-3 R1.6 is troublesome as well. Entities typically use update or proxy servers to discover and identify applicable security patches. For example, we use Windows Update Server Services to identify patches and roll them out once testing and approvals are complete. Do we need to check the check sums of the identified patches or can we trust that the update servers are authenticating the software?

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment
The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” USI has concerns with R 1.6.1 and 1.6.2 as written about how to provide evidence? Therefore, we believe more examples of evidence should be provided. While we support these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	

Comment
GSOC supports NRECA's Comments of: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: “For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer.” This sentence seems to be incomplete and further words are needed to complete it.

Likes 0	
Dislikes 0	

Response

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment

R1.6 brings to mind several challenges. The intent appears to be to ensure that software is validated, which is not the issue. The issue is the auditability of the requirement and its existing language. The wording “when the method to do so is available” puts additional obligations on the Responsible Entity to prove whether the methods were available or not, when the methods were available, if it was appropriate to utilize the available methods in a given circumstance. It adds additional nuance when the methods are often obtained from third parties. If it is a legacy contract and has not been updated and the method is available to other entities but not to the Responsible Entity due to the legacy contract, is the method considered available? The intent of this requirement is good but the auditability of the language is challenging at best and should be adjusted to consider how entities will be able to document and comply with the requirement language.

Likes 0	
Dislikes 0	

Response

Heather Morgan - EDP Renewables North America LLC - 5

Answer	Yes
Document Name	

Comment

- Please provide clarification to what, “verification of identity of the software source and integrity of the software” means. Please provide more examples within the Measures to ensure entities are prepared for compliance oversight expectations.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	Yes
Document Name	

Comment

MMWEC supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	Yes

Document Name	

Comment

SPP recommends that the drafting team provide examples to provide clarity on control design to meet the intent of the standard.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

NRG recommends that the drafting team provide examples to provide clarity on control design to meet the intent of the standard.

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. NRG requests guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

The VSL as currently written may not cover the failure to implement the process. The VSL may not include all of the combinations.

NRG has concerns with Parts: 1.6.1 and 1.6.2 as written --- For example, how would a Registered Entity be expected to provide evidence? NRG request additional examples of evidence in the Measures section of the requirement.

NRG suggests rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” may be ambiguous and leaving the following questions:

How does one prove that a method is not available?

What is the line between available/unavailable? How far do you have to go?

NRG is concerned with double jeopardy potential with CIP-007 R2. NRG is concerned that it may be difficult or impossible to validate the source or verify authenticity of the patch itself which may cause the industry to not consider that patch to be available.

Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
ITC Holdings believes the wording of CIP-010-3 leaves a lot of room for interpretation and needs to be more prescriptive. The measures should define technical examples (e.g., denote MD5 fingerprint or hashing as being an acceptable method). Additionally, ITC recommends including Remedy in the Technical Guidance document if you can't use the file integrity method.	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	

Document Name	

Comment

Texas RE notes that the proposed standard is not responsive to the FERC directive. FERC Order No. 829 P. 59 specifically states "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." The Note in Part 1.6, however, states: "Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual *terms and conditions of a procurement contract*; and (2) vendor performance and adherence to a contract." Texas RE agrees that it is unreasonable to hold a registered entity accountable for a vendor's adherence to (or lack of adherence to) a contract. Texas RE agrees as the SDT claims obtaining specific controls in the negotiated contract may not be feasible at all times but Texas RE believes this is *best practice*. In fact, in most cases contracts for these types of systems typically include security provisions and set similar expectations as described in the standard. The proposed standards would prohibit the compliance monitor from verifying the registered entity implemented part 1.6. Moreover, this verification is to ensure that the registered entities' plans are consistent with the contract's expectations and obligations of the parties.

Admittedly, there will be circumstances in which a contracts may not be consistent or silent as it pertains to the responsible entity's security management plans (e.g. existing contacts or contracts in which the responsible entity was unable to negotiate the appropriate terms into the contract.) In those circumstances, other evidence should be provided demonstrating that the responsible entity has processes to ensure the vendor is expected/obligated to act consistent with the responsible entity's cyber security risk management plans as it relates to the vendor's products or services. Therefore, the contracts should remain in scope as to demonstrate the mapping of expectations from the plan to the contract as far as vendor interactions for those specific items included in the standard and to advance best practices leading to a more reliable BES.

Texas RE also recommends the SDT remove or provide clarity on the verbiage that reads, "*and when the method to do so is available to the Responsible Entity from the software source*". A potential scenario exists now where vendors will attest that identity and integrity methods are not available therefore Part 1.6 is not applicable.

Texas RE notes that the words "integrity" and "authenticity" are used in the Guidelines and Technical Basis however Part 1.6 uses the words "identity" and "integrity". Are these intended to be the same?

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power

Answer	
Document Name	

Comment

MEAG supports the answers and comments of Salt River Project.

Likes 0	
Dislikes 0	

Response

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response	

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx
Comment	
Malware inserted into the U.S. electric grid in year 2014 and into the electric grid and other assets in the Ukraine in December 2015 and December 2016 target nominally "low impact" assets producing high impact consequences. See integrated comments that address in part the need to upgrade protections for so-called "low impact" facilities.	

Likes 0	
Dislikes 0	

Response

David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG

Answer	No
Document Name	

Comment

While the IRC members do not have Low Impact Bes Cyber Systems we have multiple interfaces with our Market Participants that do have Low Impact BES Cyber Systems. This, in turn represents, risk to our BES Cyber Systems. As such we recommend that CIP-013-1 apply to Low Impact BES Cyber Systems to reduce the supply chain risk not only to the Low Impact BES Cyber Systems but to the IRC member organization's BES Cyber Systems.

Note: **PJM does not support this comment**.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10

Answer	No
Document Name	

Comment

While the initial direction of CIP-013-1 is good and provides protection for High BCS and Medium BCS, similar Cyber Assets associated with Low impact BES Cyber Systems may represent vectors for attack to High BCS or Medium BCS if left unprotected. WECC understands the reluctance of industry to incorporate Low impact BCS and their component BCA and other Cyber Assets under the CIP-013-1 purview and supports remanding SCRM issues associated with Low impact BCS to the CIP-003 Standard Drafting Team for integration into R1.2 and R2 of that Standard to ensure SCRM is integrated into those BCS at a level commensurate with the risk posed to the reliability of the BES.

Likes 0	
Dislikes 0	

Response

Franklin Lu - Snohomish County PUD No. 1 - 6

Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	

Comment
Oxy agrees with the removal of low impact BCS from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. Oxy believes that for entities that have a mixture of high, medium and low impact assets, the low impact assets would inherently benefit from the requirements applicable to high and medium impact assets as a matter of normal business practice, as the high water mark will be applied when purchasing equipment and services. This will account for a large portion of low impact BES Cyber Systems. Oxy believes it is appropriate to address the supply chain requirements using this risk-based approach. Low impact BES Cyber Systems are categorized as low impact because they inherently pose a low risk to negatively impact the Bulk Electric System. Resources should focus on those systems that have the potential for significant adverse impact on the BES. Additionally, vendors will not differentiate their product as low, medium or high impact, so as vendors address the requirements of high and medium impact entities, low impact entities will acquire the same products and services as medium and high impact entities. If low impact BES Cyber Systems were included in CIP-013-1, the costs associated with compliance would far outweigh the risk posed to the BES, in both manpower and additional equipment and services.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment
No additional comments.

Likes 0	
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	

Comment
GTC supports NRECA comments: NRECA appreciates the SDT's efforts to develop the supply chain requirements under a risk-based lens.

Likes 0	

Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
None	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes. Industry supply chain management advances that would impact low impact BES Cyber Systems would be addressed by vendors through the requirements for high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the removal of low-impact BES Cyber Systems from the applicability of CIP-013-1. Low-impact BES Cyber Systems have been subject to a risk assessment and classified low-impact since they pose a minimal threat to the BES. Also, a Responsible Entity is not required to have an inventory list of its low-impact BES Cyber Systems. If this standard were to apply to low-impact BES Cyber Systems, this would likely create a situation wherein an inventory list is necessary. This would be a significant effort, which would not likely bolster the reliability of the grid, based on the limited impact lows present to the system.	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE appreciates the SDT’s efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Luminant believes it is appropriate to address the supply chain requirements using a risk-based approach. Low impact Cyber Systems are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES. In addition, there are many types of low impact Cyber Systems. If a decision was made to put them back into the standard, there would need to be extensive work on evaluating each of these types of systems in order to determine whether there is adequate benefit to reliability to offset the cost and burden of imposing supply chain requirements for these systems.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
IPC agrees that the applicability to Lows should be removed.	
Likes 0	
Dislikes 0	
Response	

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA appreciates the SDT’s efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
USI agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agree that the current standard as written appropriately addresses the Commission’s concerns as specified in Order No. 829.	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
NPPD supports the position of the MRO NSRF.	
Likes 0	
Dislikes 0	
Response	

David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA appreciates the SDT’s efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	

SRP agrees with the removal of low impact BCS from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. SRP believes that for entities that have a mixture of high, medium and low assets, the low assets would inherently benefit from the additional requirements of medium and low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have low assets only, there would not be additional requirements based on CIP-002 risk based approach.

SRP believes that including lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with lows.

Likes 0	
Dislikes 0	
Response	

Normande Bouffard - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	

No comments

Likes 0	
Dislikes 0	
Response	

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	

See Attached Comments.

Likes 0	
Dislikes 0	
Response	

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro believes that focussing on Medium and High Impact BCS instead of Low Impact is a good place to start. If insufficient risk mitigation is found to be provided here, it can always be expanded later. However, BC Hydro does not believe CIP-013-1 itself is necessary given what entities will already be doing under the other CIP v5 standards	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE agrees with removing low-impact BCS from CIP-013-1 and agrees the current standard, as written, appropriately addresses the Commission's concerns as specified in Order No. 829. AE believes, for entities with a mixture of High, Medium and Low Impact BCS, the Low Impact B CA would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many contracts and master agreements are developed for all products and services purchased from a vendor. For entities with Low Impact BCS only, there would not be additional requirements based on the CIP-002 risk-based approach. AE believes including Low Impact BCS will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these devices. Also, controls inherent to CIP-013 and previous CIP Standards reduce the risk associated with Low Impact BCS.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

SMUD agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. SMUD believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach.

SMUD believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with Lows.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

PRPA agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. PRPA believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach.

PRPA believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with Lows.

Likes 0	
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5

Answer	Yes
Document Name	

Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees with the removal of low-impact BES Cyber Systems from CIP-013-1. Including low-impact BES Cyber Systems will require substantial resources by a Responsible Entity it identify and maintain an inventory list of items.	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	

Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	

Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes

Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE's opinion is that low impact BES Cyber Systems should be included in CIP-013-1 because industrial control systems monitor and operate BES Cyber Assets located at transmission substations, wind farms, and generation facilities.

Texas RE noticed that Question 4 uses the words "hardware, computing and networking services", which are not found in CIP-013-1. Should they be used in CIP-013-1 instead of "equipment, products, and services"?

Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance

Answer	
Document Name	

Comment

No comment

Likes 0	
Dislikes 0	

Response

Mark Holman - PJM Interconnection, L.L.C. - 2

Answer	
Document Name	

Comment

PJM chooses to abstain from this question as we have no low impact assets.

Likes 0	
Dislikes 0	

Response

Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power

Answer	
Document Name	

Comment
MEAG supports the answers and comments of Salt River Project.

Likes 0	
Dislikes 0	

Response

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

Gregory Campoli - New York Independent System Operator - 2

Answer	No
Document Name	

Comment

Request a 24 month implementation due to budget cycles and technical controls for other CIP Standards.

Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance

Answer	No
Document Name	

Comment

Disagree with the Implementation Plan. Standard should have language stating whether or not software installed prior to enforcement must have identify/verification completed.

Likes 0	
Dislikes 0	

Response

Timothy Reyher - Eversource Energy - 5

Answer	No
Document Name	

Comment

Recommend changing this General Consideration from

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note

Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.

Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion

Answer	No
Document Name	

Comment

Recommend changing this General Consideration from

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note

Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.

Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards

Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
Performance requirements are too vague to be auditable. See related comments.	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	
SMUD generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. SMUD feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers. SMUD is indicating a “no” response as the implementation plan does not include a pilot. The implementation of TCA CIP 010 R4 was difficult as entities did not have a model implementation to learn practical applications of the standard in operations. Other standards that had a pilot allowed entities to learn practical implementation decisions that would save money and time. Please note, SMUD is willing to participate as a pilot participant.	
Likes 0	
Dislikes 0	
Response	

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

It is uncertain when purchasing activities become subject to CIP-013-1. The proposed Implementation Plan states: “Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.”

Reclamation recommends that the “General Considerations” guidance contained in the Implementation Plan pertaining to purchasing activities be included in the proposed standard.

If the “General Considerations” guidance on purchasing activities becomes part of the proposed standard, Reclamation further recommends:

- A contract becomes within scope when the entity commences its formal contract process such as when a request for proposal or solicitation is issued.
- Any direct purchase and/or any repurposed equipment is within scope prior to connecting to the Bulk Electric System as a cyber asset.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

CIP-013 R2 and/or the Implementation Plan should contain “trigger” language for R2 that clarifies an entity must implement its R1 risk management plan(s) for new procurement contracts signed on or after the Effective Date of CIP-013. Entities with no new procurement contracts or no new in-progress procurements on the Effective Date should not be expected to be able to demonstrate compliance with R2 at that time.

Likes 0	
Dislikes 0	
Response	

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No

Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24-month implementation due to budget cycles and technical controls for other CIP Standards	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To	

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note

Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.

Likes 0	
Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3

Answer	Yes
Document Name	

Comment

FEUS supports the comments submitted by APPA

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski

Answer	Yes
Document Name	

Comment

GRE and the NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the “Planned or Unplanned Changes Resulting in a Higher Categorization” section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan.

Additionally, the absence of the “Applicable Facilities” section or other language that clearly indicates these standards/requirements do not apply to “low” entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	Yes
Document Name	
Comment	
Yes. Moving the implementation date from 12 to 18 months is consistent with the CIP v5 implementation timeline for implementations. Would low impact BES Cyber Assets that might be in scope in the future have similar implementation timeline or longer?	
Likes 0	
Dislikes 0	
Response	

Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts

Answer	Yes
Document Name	
Comment	
AECI supports NRECA's comments provided below: NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the “Planned or Unplanned Changes Resulting in a Higher Categorization” section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the “Applicable Facilities” section or other language that clearly indicates these standards/requirements do not apply to “low” entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	
Likes 0	
Dislikes 0	
Response	

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments:	

NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan.

Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.

Likes 0	
Dislikes 0	

Response

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Southern recommends that the SDT consider addressing previous issues with the Implementation Plan versions between CIP V5, V6, V7, etc., where Implementation Plans were "chained" together and there was not an Implementation Plan that contained all the necessary requirements in a single source. Southern strongly recommends producing a consolidated Implementation Plan.

Southern recommends that NERC and the SDT(s) consider addressing issues with the Implementation Plan versions between CIP V5, V6, V7, and Supply Chain, as Implementation Plans are "chained" together and there is no one Implementation Plan that contains all the necessary requirements in a single source. Implementation Plans for the CIP standards cover several important areas:

Implementation schedules of new or modified CIP standard requirements.

Implementation schedules for newly identified cyber assets brought into scope with current requirements based on planned or unplanned changes in the BES assets, or those from newly registered NERC entities. (previously known as IPFNICANRE – Implementation Plan for Newly Identified Cyber Assets or Newly Registered Entities)

Implementation schedules for BES Cyber Systems already in scope that change impact levels due to planned or unplanned changes in the BES.

As an example, the last page of the Implementation Plan for CIP-003-7 states that CIP-003-6 is retired upon approval of CIP-003-7, yet it chains to the CIP-003-6 Implementation Plan to tell entities how to handle cyber systems that change impact categorization. The CIP-003-6 implementation plan simply says it replaces *parts* of the V5 implementation plan for the modified standards in that revision. Only the V5 plan addresses the 2nd bullet point above. Responsible Entities are left to unravel three different plans with supply chain adding yet another to get one picture of what is due when and knowing how to handle BES changes that affect cyber system identification and impact categorization.

As we go forward, we need a better solution. Parts of an implementation plan, such as bullets 2 and 3 above, need to live on indefinitely. Other parts, such as the schedule of new or modified requirements, need to live until those dates have passed. Chaining all of this together through numerous documents as the CIP standards continue to evolve and grow to cover new areas is not a sustainable solution that promotes clarity in knowing the compliance obligation in a changing environment.

Likes 0	

Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Disagree with the Implementation Plan. Standard should have language stating whether or not software installed prior to enforcement must have identify/verification completed.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	

Dislikes 0	
Response	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	

Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
As mentioned above, WECC supports the CIP-013-1 implementation plan, including the expectation for the initial performance of the R3 review and approval on or before the effective date.	
Likes 0	
Dislikes 0	
Response	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	

Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	

Comment
We agree with APPA's submitted comments, including: Suggesting a change in wording to say that the Supply Chain Risk Management Plan must be used on or after the implementation date rather than saying that contracts on or after that date are within scope of CIP-013. Clarification should be made about if/when existing contracts or agreements come into scope.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	

Comment
PRPA generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. PRPA feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	

Comment
AE generally agrees with an 18-month implementation plan but, would prefer 24-months. AE feels a 24-month timeframe is more appropriate and gives entities additional time to align budgets and develop processes with vendors and suppliers. As a municipal utility, AE's procurement process is quite long.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date of the CIP-013-1. Make corresponding change to the CIP-013 R2 note. And CIP-005-6 and CIP-010-3 must be implemented 18 months after the implementation date of the CIP-013-1 Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24 month implementation of CIP-013-1 due to budget cycles and technical controls for other CIP Standards	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
SRP generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. SRP feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While in overall agreement with the updated Implementation Plan, ACEC does have the following concern: The second paragraph in the section “General Considerations” states “Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.” Based upon the above wording it could be understood that Master Supply Agreements (MSAs) would need to be changed in the first RFP after implementation of the new standard. The paragraph should state specifically that this is not required, and that the plan can allow MSAs to exist as is until it is time to review in the normal procurement process.	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the “Planned or Unplanned Changes Resulting in a Higher Categorization” section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the “Applicable Facilities” section or other language that clearly indicates these standards/requirements do not apply to “low” entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	

Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Thank you for your statement under Initial Performance of Periodic Requirements, that the supply chain security risk management plans need to be approved on or before the effective date of CIP-013-1.	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Comments: NPPD supports the position of the MRO NSRF. NPPD believes a 24-month implementation should be used due to budgeting and tthe technical implementation requirements for the other CIP Standards.	

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4

Answer	Yes
Document Name	

Comment

Recommend changing this General Consideration from:

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To:

Supply Chain Risk Management plan must be used by appropriate procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note.

Further, USI requests clarification on if/when existing contracts, master contracts, or long-term maintenance agreements that re-opened for renegotiation or put in use, come into the scope of CIP-013.

The implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request that the Implementation Plan be modified to handle entities that meet the applicability after the effective date of the standard.

USI believes a 24-month implementation should be used due to budget cycles and technical controls for other CIP Standards.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 4

Answer	Yes
Document Name	

Comment

GSOC supports NRECA's Comments of:

NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the

language from the “Planned or Unplanned Changes Resulting in a Higher Categorization” section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan.

Additionally, the absence of the “Applicable Facilities” section or other language that clearly indicates these standards/requirements do not apply to “low” entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	Yes
Document Name	

Comment

NRG recommends changing this General Consideration from:

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Please consider making the corresponding change to the CIP-013 R2 note

The Implementation Plan does not appear to address unplanned changes such as IROLs or registration, etc.

NRG requests consideration of a 24 month implementation due to budget cycles and technical controls for other CIP Standards

Likes 0	
Dislikes 0	

Response

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	

Answer	
Document Name	
Comment	
Texas RE requests that the SDT provide its rationale for extending the effective date from 12 to 18 months. For example, it is unclear whether the SDT believes more certainty is required regarding the necessary technical deployments for compliance with the Standard as some commenters suggested to justify the extended implementation period.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response	

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment

ERCOT joins the comments of the IRC.

Likes 0	
Dislikes 0	

Response

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment

Duke Energy suggests the drafting team consider implementing a staggered approach to the VSL(s) specifically to CIP-013-1 R2. As written, an entity could implement all aspects but one sub-part of the risk management plan, and the violation would have a VSL of Severe. We recommend the drafting team consider a more equitable approach and stagger the VSL(s) similar to the approach used in R1 of CIP-003-6.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

MMWEC supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

We do not agree with the VRF Justification for CIP-013-1 R1, FERC VRF G5 with the new redline. Agree with the words that were redline out.

CIP-010 – VSL does not cover the failure to implement the process and therefore does not include all of the combinations. Consequently, we request that there be lower severity levels when a single aspect of the requirements is missing.

Request that that the term “elements” be included in CIP-013 R1.2 (as shown in comments for question 1) to clearly align with the VSLs for this requirement.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	

See attached comments

Likes 0	
Dislikes 0	

Response

Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

The VSL for R2 only provides for a Severe VLS. It is unclear what is meant by "did not implement". If your plan has 5 areas within it and 4 of the 5 were fully implemented, has the plan been implemented? I contend yes however not fully implemented. The VSL were created to identify how far of the complaince mark an entitiy fell. This VLS completly fails to perform this action. While at the same time the VSL for R3 utilizes arbitrary calendar months

for clear VLS seperation between lower and severe. Both of these VLS provide little benefit to industry in assessing the real impact to the BES based on an entity missing the complaince mark.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
We support APPA's comments that the original wording is better than the new redline of the VRF justification.	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
While an important topic, at this time AEP does not agree that risks associated with violations of these draft standards is a “Medium” risk to the BES. AEP recommends the Violation Risk Factor for each of the requirements CIP-013-1 R 1-3 be considered “Lower.”	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement.

“***1.2.*** *One or more process(es) for its newly procured BES Cyber Systems that address the following elements, as applicable:”*

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

: For CIP-013-1, R3, Dominion recommends the following alternate VSL values.

- Low – No change
- Moderate – 16-18 calendar days
- High – greater than 18 calendar days
- Severe – When a review has never been performed

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	

Comment

CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement.

“***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:”*

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:”*	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:”*	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	No
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	

Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	

Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The IRC suggests the drafting team add more thresholds to the VSLs for R2 of CIP-013-1 and that it be aligned more closely with that of R1, rather than making it binary. The cyber security risk management plan will be fairly large and missing small portions of the plan should not immediately result in a Severe VSL.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	

Answer	Yes
Document Name	
Comment	
None	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	

Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
There should be lower, moderate and high VSLs for R2, (not implementing portions of the requirement). PJM suggests using the language in the lower, moderate and high R1 VSLs as a starting point.	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Yes for CIP-005-6 and CIP-010-3 only	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

None	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
YES for CIP-005-6 and CIP-010-3 only	

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP agrees with the VRFs and VSLs for CIP-010 and CIP-013. SRP believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to determine and did not have a method to disable. SRP would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable.

SRP requests that the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	Yes
Document Name	

Comment

AE agrees with the VRFs and VSLs for CIP-010 and CIP-013. AE believes the VRFs and VSLs for CIP-005 should be updated to reflect the same approach taken in CIP-010. The VSL for CIP-005 results in a severe penalty if an entity does not have a method to determine and does not have a method to disable. AE would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable.

AE requests the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of

Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
SMUD agrees with the VRFs and VSLs for CIP-010 and CIP-013. SMUD believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to determine and did not have a method to disable. SMUD would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. SMUD requests that the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
PRPA agrees with the VRFs and VSLs for CIP-010 and CIP-013. PRPA believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to determine and did not have a method to disable. PRPA would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. PRPA requests that the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response	

Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No Comment.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
WECC has no issues with the VSLs or VRFs from a CIP Auditor perspective.	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	

Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response

Andrew Meyers - Bonneville Power Administration - 6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response	

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	No
Document Name	
Comment	
The requirements aren't vetted enough to make a fair judgement.	
Likes 0	
Dislikes 0	
Response	

Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	
Implementation Guidance for R3 Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing "Below are some examples of approaches to comply with this requirement:" to "Below is an example of an approach to comply with the review requirement required by:" Implementation Guidance for R3 – Recommend removing this language from the second main bullet, since it is beyond the Requirement "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed."	
Likes 0	
Dislikes 0	
Response	

Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	No
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.	
Likes 0	

Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	

Comment
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	

Comment
The existing guidance still provides no scope of cyber security risks that should be considered, and without context, many of the proposed actions have no guidelines or measurements for “success” or “failure” or acceptability; nor are there suggested acceptable mitigations if a criterion is not completely met, since there is no clear objective. Furthermore, there is no allowance made for a continuous process, where, as a result of products already being used in BES Cyber Systems and subjected to the existing CIP standards, cyber security risks associated with networks, products and vendors are evaluated on an on-going basis. Detailed changes and additions are outlined in a separate redline Draft Implementation Guidance document that has been forwarded to NERC and the SDT. A summary of the proposals is as follows: 1. Throughout the document, the term ‘controls’ should be changed to a term that more closely reflects the language in the proposed standard. Dominion recommends using ‘terms and conditions’. 2. On page 2, dominion recommends clarifying that cyber security risks are limited to supply chain with the addition of ‘supply chain’ prior to each use of the term cyber security risks. 3. In addition to the clarifying language in item #2 above, Dominion recommends adding the following to more clearly define the term ‘supply chain cyber security risk: (1) procuring and installing un-secure equipment or (2) procuring and installing un-secure software, including purchasing counterfeit software, or software that has been modified by an un-authorized party, (3) unintentionally failing to anticipate security issues that may arise due to network

architecture, (4) unintentionally failing to anticipate security issues that may arise during technology and vendor transitions for BES Cyber Systems). The additional bullets could be sub-bullets under the appropriate of these four broad areas as examples rather than individual, isolated items.

4. Dominion recommends deleting the third paragraph on page 2. This paragraph appears to be creating new/different obligations. The language appears to create confusion and calls out Section 1.2.5 specifically for no apparent reason.

5. The language in blue boxes throughout the document should be retained and included in the text of the document.

6. It is unclear what the purpose of including certain language in a blue box is.

7. Section headings should be included with each of the examples. Also, the bulleted format makes it unclear if one, all, or a certain number of bulleted items need to be performed to achieve compliance.

8. Add the following example under R1.1:

Develop an approved vendor/products list. When planning a BCS, the RE should evaluate the following items:

-
    - Vendors
    - Products
    - Network Architecture
    - Network Components.

The RE should document (which may be limited to the baseline and cyber vulnerability assessment (CVA) required for a new product) any risks (i.e. 1) procuring and installing un-secure equipment or (2) procuring and installing un-secure software, including purchasing counterfeit software, or software that has been modified by an un-authorized party, (3) unintentionally failing to anticipate security issues that may arise due to network architecture, (4) unintentionally failing to anticipate security issues that may arise during technology and vendor transitions for BES Cyber Systems) identified and how the risks are mitigated for any “item” that deviates from those vendors, products, network architecture, and network components already being used within the RE’s BCS infrastructures, which are required to comply with existing CIP standards.

9. The second bullet in Section 1.2.2 should be removed. It is already addressed under Section 1.2.1.

10. In Section 1.2.3, the end of the first bullet could state be clarified as follows:

Delete ‘within a negotiated period of time of such determination’ and replace with “to allow the RE to remove access within 24 hours of the determination, consistent with existing CIP standards”

Replace ‘breaches’ with ‘vulnerabilities’ for clarity and consistency’.

Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
The Implementation Guidance only identifies items that could be evaluated in developintg a Supply Chain Cyber Security program, but does not provide an example or guidance on how to implement the program. Without this guidance, it is impossible to understand how to comply with CIP-013-1 in a cost-effective and compliant manner.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	

We agree with APPA's submitted comments concerning "vendor" not being a NERC-defined term and that the Implementation Guidance for R3 does not adequately explain compliance needs.

Likes 0	
Dislikes 0	

Response

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro

Answer	No
Document Name	

Comment

BC Hydro does not agree with the examples as compliance will be challenging. It would require us to have sufficient authority over the vendor (which will not be the case in most situations). There is also no way to ensure that a vendor is being completely transparent regarding cyber vulnerabilities in their product. Such disclosure could have other impacts on their business with other clients. This would be a dis-incentive for disclosure. BC Hydro does not believes CIP-013 is necessary and cyber control is already achieved with the rest of the CIP v5 standard requirements around change control, testing and ongoing systems monitoring.

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	No
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment

See attached comments.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5

Answer	No

Document Name	

Comment

It is uncertain when purchasing activities become subject to CIP-013-1. The proposed Implementation Plan states: “Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.”

Reclamation recommends that the “General Considerations” guidance contained in the Implementation Plan pertaining to purchasing activities be included in the proposed standard.

If the “General Considerations” guidance on purchasing activities becomes part of the proposed standard, Reclamation further recommends:

- A contract becomes within scope when the entity commences its formal contract process such as when a request for proposal or solicitation is issued.
- Any direct purchase and/or any repurposed equipment is within scope prior to connecting to the Bulk Electric System as a cyber asset.

Likes 0	
Dislikes 0	

Response

Tho Tran - Oncor Electric Delivery - 1 - Texas RE

Answer	No
Document Name	

Comment

There is inconsistency between the Implementation Guidance and CIP-010, R1. The requirement states “For 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”. The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

The requirement wording suggests it applies for any change but the Guidance suggests that for some changes, such as patches, it would not apply. Oncor believes that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore, it is believed that the best solution is to modify the Guidance.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

USI believes the SDT should provide guidance regarding the use of the term “vendor.” If “Vendor” is not defined by NERC, the Guidance should recommend that Entities include their definition of “vendor” in their plan(s).

Implementation Guidance for R3

Neither main bullet meets compliance because both only deal with the review and not the approval. Therefore, USI recommends changing: ”Below are some examples of approaches to comply with this requirement: “ to “Below is an example of an approach to comply with the review requirement required by: “

In addition, we recommend removing this language from the second main bullet, since it is beyond the Requirement:

“Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

Also, there should be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response	

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

- The language within the Implementation Guidance contradicts the language within CIP-013. (i.e. System-based approach). The Implementation Guidance is not auditable, however, the Standard and Requirements are. EDPR NA suggests that the Implementation Guidance is eliminated and further support are provided within the Measures for a Registered Entity and auditor’s reference.
- There are numerous items in which vendors will not provide information on unless an entity is willing pay significant increases (risks, training, methodologies, threats, etc.)
- EDPR NA also suggests that NERC utilize a pilot program to test these requirements prior to enforcing the implementation of CIP-013 to all Registered Entities.

- Please provide more support with respect to the expectations and possible evidence for Requirement 2.

Likes 0	
Dislikes 0	

Response

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5

Answer	No
Document Name	

Comment

MMWEC supports comments submitted by APPA.

Likes 0	
Dislikes 0	

Response

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group

Answer	No
Document Name	

Comment

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states, in relevant part, “For 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.”

The Guidelines and Technical Basis section heading “Software and Authenticity,” paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application.

Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. SPP recommends that the SDT review the Guidelines and the draft standard for consistency and resolution.

In addition, SPP recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines.

SPP notes that there is no corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.

Likes 0	
Dislikes 0	

Response

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	No
Document Name	

Comment

NRG has concerns that the Implementation Guidance for R3 (main bullet) may not meet compliance because both only deal with the review and not the approval. NRG recommends that the NERC SDT consider changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:”

NRG has concerns that the Implementation Guidance for R3 – (specifically):

“Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

Therefore, NRG recommends that the NERC SDT consider removing this language from the second main bullet, since it is beyond the Requirement.

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states, in relevant part, “For 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.”

The Guidelines and Technical Basis section heading “Software and Authenticity,” paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update

once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application.

Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. NRG recommends that the SDT review the Guidelines and the draft standard for consistency and resolution.

In addition, NRG recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines.

NRG notes that there is no corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.

Likes 0	
Dislikes 0	

Response

Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin

Answer	No
Document Name	

Comment

ITC Holdings agrees with the below comment submitted by SPP:

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states, in relevant part, "For 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."

The Guidelines and Technical Basis section heading "Software and Authenticity," paragraph three on page 39, states: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application.

Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. SPP recommends that the SDT review the Guidelines and the draft standard for consistency and resolution.

In addition, SPP recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines.

SPP notes that there is no corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Mark Holman - PJM Interconnection, L.L.C. - 2

Answer	Yes
Document Name	

Comment

As stated in the CIP-013 comments in question 1 above, the guidance needs to clarify what constitutes an incident (such as only actual breaches).

Likes 0	
Dislikes 0	

Response

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

Yes, and BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of “policies,” not “plans.” In

Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.

Likes 0	
Dislikes 0	

Response

Jesus Sammy Alcaraz - Imperial Irrigation District - 1

Answer	Yes
Document Name	

Comment

The understanding of the intent and purpose of CIP-013 is very dependent on the Implementation Guidance document. We are concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such we would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.

Likes 0	
Dislikes 0	

Response

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	

Comment

The Guidance for CIP-013-1 R3 should include the term 'approved' since an Entity wouldn't comply with the requirement with just a review.

Likes 0	
Dislikes 0	

Response

Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes, the Compliance Guidance policy does provide industry with direction for implementation. However, those guidance details are not written in the requirements, measures or Reliability Standard Audit Worksheet (RSAW) and cannot be relied upon in preparation of an audit. ACES would suggest, at a minimum, that these guidelines be written in the Supply Chain Management RSAWs in the section 'Notes for an Auditor'. By placing this information in the RSAW, it gives industry additional reassurance that each region will audit Supply Chain Management consistently.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Implementation Guidance for R3 Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing "Below are some examples of approaches to comply with this requirement:" to "Below is an example of an approach to comply with the review requirement required by:" Implementation Guidance for R3 –	

Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response

Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1

Answer	Yes
Document Name	

Comment

Implementation Guidance for R3

Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:”

Implementation Guidance for R3 –

Recommend removing this language from the second main bullet, since it is beyond the Requirement

“Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

Likes 0	
Dislikes 0	

Response

Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates

Answer	Yes
Document Name	

Comment

For consistency and clarity between sub-requirement 1.2.2. and the CIP-013-1 Implementation Guidance, we suggest that “cyber security incident(s)” be removed from the examples for 1.2.2. This verbiage should be replaced with either “vendor-identified incidents” or “security event(s)” as referenced in the examples for 1.2.1.

Likes 0	
Dislikes 0	

Response

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
The guidance relative to R1.2.2 and R1.2.6 partially address WECC's concerns as stated in Bullet 2 above. In general, the example approaches provide good guidance to industry on ERO expectations for compliance with the various Requirements and Parts. No other issues noted.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
The intent and purpose of CIP-013 is very dependent upon the Implementation Guidance document. We appreciate the hard work of the SDT to provide this document to industry and it has valuable information. Additionally, there is no guarantee this document will be approved by NERC.	
Likes 0	
Dislikes 0	
Response	

Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
PRPA generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. PRPA is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, PRPA would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard. R3: PRPA requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.” Request that there be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.	
Likes 0	
Dislikes 0	
Response	

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

In the guidance for Requirement R1, Part 1.2.5, CenterPoint Energy believes including all third-party hardware, software, firmware, and services goes beyond the scope of the requirement. Most systems consist of components or services from numerous third-party companies. The vendor of such systems may not have direct contact with third-party companies. The level of third-party components or services that could be expected to be included may be quite extensive and therefore make it impractical for the vendor to commit to such issues in contract provisions.

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. SMUD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, SMUD would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.

R3: SMUD requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

SMUD also requests that there be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	Yes
Document Name	

Comment

AE is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. AE has concerns about the possibilities NERC and the Regions: (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, AE would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.

R3: AE requests the following language be removed from the second main bullet, because it is out-of-scope for this Requirement:

"Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

AE requests there be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2, Parts 2.4 and 2.5 and CIP-010-3 R1.6.

Likes 0	
Dislikes 0	

Response

Normande Bouffard - Hydro-Qu?bec Production - 5

Answer	Yes
Document Name	

Comment

Make sure the Compliance Guidance is in the scope of standards.

Likes 0	
Dislikes 0	

Response

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance

Answer	Yes
Document Name	

Comment

As mentioned in previous comments, this document provides implementation guidance on CIP-013, but additional guidance on implementation of the CIP-010 and CIP-005 controls is requested, perhaps in the Supplemental Material sections. Particularly CIP-005 R2.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

SRP generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. SRP is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, SRP would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.

R3: SRP requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

Request that there be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.

Likes 0	
Dislikes 0	

Response

Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	

Yes, and BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.

Likes 0	
Dislikes 0	
Response	

Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

While in overall agreement with the Implementation Guidance for CIP-013, ACEC does have the following concern:

In the Implementation Guidance for R1 Section of the document, the subsections for implementation of Requirement R1 Parts 1.2.1, 1.2.2, 1.2.4 and 1.2.5 use the generic term "vendor(s)" in discussing these Software Authenticity and Integrity issues. To help in ensuring that these requirements are implemented in an effective manner, it is recommended that the SDT add a clarification item, noting that these requirements be addressed by the OEM providing the hardware and/or software, not a third-party such as an integrator.

Likes 0	
Dislikes 0	
Response	

Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	

Comment
N&ST has no disagreement with the example approaches contained in the Guidance but believes that while they may represent reasonable courses of action for large entities, they are likely to be far beyond the capabilities of small ones. N&ST believes an entity whose combined BES operations, OT support, and CIP compliance teams comprise fewer than 10 individuals would be hard-pressed to “form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es).” N&ST also believes, based on experience with CIP V1 – V5 cyber security training requirements, that large vendors with many BES customers will balk, sooner or later, at being asked to respond to a multitude of risk assessment requests, questionnaires, meetings, etc., each one different from the previous ones, and will instead incline towards providing a standardized set of information about their internal risk management programs and how they are applied to their products and services.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	

Comment
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment
Exelon thanks the SDT for submitting the draft Implementation Guidance for CIP-013. Does the SDT also intend the develop draft Implementation Guidance for the revised/added sections of CIP-005 and CIP-010? If so, is there a timeline that can be shared with Industry participants?

Likes 0	
Dislikes 0	

Response

Stephanie Little - Stephanie Little

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response	

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

William Harris - Foundation for Resilient Societies - 8

Answer	No
Document Name	

Comment

We consider the requirements to be burdensome, and impractical for many or most electric utilities without providing needed protection of the cyber supply chain. We would suggest at the outset adoptioon of a separate FERC rulemaking to detect, report, mitigate and remove malware from the bulk electric system.

Likes 0	
Dislikes 0	

Response

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators

Answer	No
Document Name	

Comment

By placing those comments and guidance in the Implementation Guidance does not provide industry protection during an audit in defining ‘cost effective manner’. If it is important to communicate to industry that Supply Chain Management can be managed in a ‘cost effective manner’, then that should be detailed in the standards. ‘Cost effective manner’ is an undefined term and will be different for each entity, budget and their resources. The focus should be modified to a ‘risk reduction manner’ or ‘risk appropriate manner’.

Likes 0	
Dislikes 0	

Response

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6

Answer	No
Document Name	

Comment

There is not enough clarity in the proposed language to make that assessment.

Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG is cognizant and appreciative of the flexibility provided in proposed CIP-013-1 and the draft Implementation Guidance but at this time cannot speak to whether the implementation of these requirements will be cost effective. Additional internal analysis is needed to inform NRG's evaluation as to the cost-effectiveness of the proposal.	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
SPP is cognizant and appreciative of the flexibility provided in proposed CIP-013-1 and the draft Implementation Guidance but at this time cannot speak to whether the implementation of these requirements will be cost effective. Additional internal analysis is needed to inform SPP's evaluation as to the cost-effectiveness of the proposal.	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	
By asking vendors to enforce these requirements, service costs will dramatically increase which will put a further strain on the electric industry.	

Likes 0	
Dislikes 0	

Response

Don Schmit - Nebraska Public Power District - 5

Answer	No
Document Name	

Comment

This new standard will put additional burden on entities. It is going to take considerable time to implement and negotiate new contracts. It is also up to the entity to provide adequate documentation to prove compliance but it will still be based on the auditor discretion if an entity has done enough. As with similar requirements in the nuclear industry we believe that contract pricing will increase due to the Standard requirements placed on the vendors via industry and may result in reduction of vendor options.

Likes 0	
Dislikes 0	

Response

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment

N&ST believes the approaches to meeting CIP-013's reliability objectives described in the Implementation Guidance could easily consume scores, if not hundreds, of staff hours, with the potential to make "vendor risk assessment(s)" a significant cost component of any large-scale procurement. N&ST notes that although most of the documents referenced in the Guidance document are available for download at no charge, the Shared Assessment Program's Standardized Information Gathering (SIG) questionnaire, referenced in a footnote, must be purchased for $6,000. The Guidance document does point out that a Responsible Entities are free to pursue different approaches to CIP-013 implementation that "better fit their situation," but provides no examples of alternatives that might be worth considering. N&ST encourages NERC and the SDT to consider how utilities with very small staffs and very limited budgets might reasonably address their CIP-013 obligations.

Likes 0	
Dislikes 0	

Response

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation’s position is that the determination of “cost effectiveness” will remain subjective unless a method to determine burden is consistent across the industry.	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	
Comment	
There is not enough clarity in the proposed language to make that assessment.	
Likes 0	
Dislikes 0	
Response	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro does not agree that implementing this standard will be cost effective. Costs and contract management to enforce CIP-013 on all vendors, in light of the limited authority the responsible entity would have over vendors, are anticipated to be significant. Especially, but not limited too, in situations where there is limited vendor choice for a class of product.	
Likes 0	
Dislikes 0	
Response	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
The Implementation Guidance only identifies items that could be evaluated in developintg a Supply Chain Cyber Security program, but does not provide an example or guidance on how to implement the program. Without this guidance, it is impossible to understand how to comply with CIP-013-1 in a cost-effective and compliant manner.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	No
Document Name	
Comment	
Santee Cooper believes that this standard will increase the cost of purchasing products from vendors unless the standard effectively addresses the use of regional master contracts, master agreements, and piggyback agreements. If a Responsible Entity loses the ability to utilize such contracts and agreements the aggregated buying power and large purchase discounts will be lost.	
Likes 0	
Dislikes 0	
Response	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.	

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	No
Document Name	

Comment

By not clarifying “cyber security risks” in R1 Part 1.1 the SDT is not providing flexibility, but rather compliance risk to Registered Entities. See our comments to questions 1 and 7, above, regarding the Implementation Guidance. As it stands, the document provides no guidance and raises additional, possible compliance risk as to interpretation of what “cyber security risks” are.

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	No
Document Name	

Comment

CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response

Haley Sousa - Public Utility District No. 1 of Chelan County - 5

Answer	No
Document Name	

Comment

CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response

Janis Weddle - Public Utility District No. 1 of Chelan County - 6

Answer	No
Document Name	

Comment

CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Avista agrees with the SDT’s belief that the proposed CIP-013-1 and the ERO Enterprise-Endorsed Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements. In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
We support the changes and believes that most aspects of CIP-013 may be achieved cost-effectively (if not necessarily cheaply), with two exceptions.	

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, USI strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. USI suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	Yes
Document Name	

Comment

NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	Yes
Document Name	

Comment

EEI agrees with the SDT's belief that the proposed CIP-013-1 and the ERO Enterprise-Endorsed Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements.

In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements.

Likes 0	

Dislikes 0	

Response

Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	

Comment
In the Draft CIP-013-1 – Cyber Security - Supply Chain Risk Management requirement R2 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.” With this note the Responsible Entity is basically directed to develop a plan yet it does not have to change procurement results. If you are not going to require results, there is no reason to add the costs of developing and implementing the program.

Likes 0	
Dislikes 0	

Response

Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	

Comment
SDG&E is not able to determine if the proposed CIP-013-1 and the draft Implementation Guidance are cost effective. Additional changes to existing contracts could incur significant cost increases.

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment

SRP generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, SRP strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BCS. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. SRP suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	

Response

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment

See attached comments.

Likes 0	
Dislikes 0	

Response

Andrew Gallo - Austin Energy - 6

Answer	Yes
Document Name	

Comment

AE generally agrees the entities can meet the reliability objectives in a cost effective manner with two exceptions:

(1) One exception is if the audit approach to CIP-013 effectively precludes use of regional master contracts and "piggyback" agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for: (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place of pre-negotiated master agreements, and (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these

risks, AE strongly urges that audit approach language for CIP-013 R2 be clarified to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

(2) Implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BCS. Some legacy cyber systems are inherently structured and configured for vendor access and reworking them to allow real-time changes may degrade system performance. AE suggests the option for a Technical Feasibility Exception be allowed for legacy systems or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	

Response

Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, SMUD strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the

performance of these systems. SMUD suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	

Response

Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill

Answer	Yes
Document Name	

Comment

SDG&E is not able to determine if the proposed CIP-013-1 and the draft Implementation Guidance are cost effective. Additional changes to existing contracts could incur significant cost increases.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

PRPA generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, PRPA strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. PRPA suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
We support APPA's submitted comments regarding the cost-effectiveness of CIP-013, pointing out two exceptions.	
Likes 0	
Dislikes 0	
Response	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Note – Comments from EEI follow: “EEI agrees with the SDT’s belief that the proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements.	

In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements. “	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
WECC concurs the draft of CIP-013-1 and the draft Implementation Guidance provide the flexibility sought by industry in its collective comments to the first ballot.	
Likes 0	
Dislikes 0	
Response	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Implementing action plans to meet reliability objectives should be cost effective, but cost effectiveness is different for each entity. Reasonable expectations of what's determined as "cost effectiveness" should be considered on an individual utility/entity basis.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	

Comment	
No comment	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	

At this point of the project, it is too early to comment on cost effectiveness. Exelon does not predict that the implementation of CIP-013 will require significant investment. However, implementing tools and processes for the revisions to CIP-005 and CIP-010 may require project management oversight as well as material financial investment.	
Likes 0	
Dislikes 0	
Response	

9. Provide any additional comments for the SDT to consider, if desired.	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	
Document Name	
Comment	

The current version of the cybersecurity supply chain standard provides a starting point for advancing controls to mitigate the risks associated with vulnerabilities in the supply chain. PJM Interconnection, LLC ("PJM") is supportive of this proposed standard as a first step consistent with the overall direction provided by the FERC.

PJM wishes to point out that the proposed supply chain standard needs to further evolve through subsequent iterations based on additional experience and incorporation of best practices. Although PJM recognizes the limits of FERC's jurisdiction as it relates to suppliers to owners and operators of the bulk electric system, any effective supply chain management standard should work to create incentives for improved cybersecurity practices up the supply chain and not just place requirements on the end user (in this case the owner or operators of bulk electric system assets). Although not evident on its face, PJM is hopeful that the proposed Standard will adequately and timely incent that goal. However, as a first step, the impact of the proposed standard, once implemented, should be analyzed with this goal in mind.

In order for supply chain risks to be substantially mitigated it will require broader cross sector engagement, broad government engagement and a significant shift in how vendors and service providers deliver products and services. Broader engagement is also required to ensure an equitable allocation of liabilities and costs. Eventually vendors and service providers will differentiate themselves by how well they manage cybersecurity risks and meet these customer needs in a fair and responsible manner.

Directionally, the proposed cybersecurity supply chain standard was intended to address a broad range of technologies as opposed to a narrower view of Energy Management and Market Management System vendors. The FERC directive similarly appeared to drive this approach. By making this choice of applying the standard to a broader range of technologies the standard, almost by necessity, starts with a more general approach with is not overly prescriptive and is grounded on the principle that organizations must establish cybersecurity supply chain processes and then execute against those processes.

The standard could have been much more prescriptive had it taken a narrower approach focusing primarily on SCADA Systems, Energy Management Systems, and Market Management Systems software solutions. Clearly the more narrow approach would have allowed for additional focus on those systems most critical to ISO/RTO operations where more proscription could have been helpful to drive more specific cybersecurity controls up the supply chain. Whether a broad approach as chosen by the drafting team or a more targeted approach is better as a starting place can be legitimately debated. In any event, either can provide a starting point for making improvements in managing the cybersecurity supply chain threats. PJM believes this effort meets that initial 'out of the gate' requirement given the need for compliance with the FERC Order in a discrete time period.

Support of the cybersecurity supply chain standard will provide an incremental step in achieving our objective of significantly improving the risks associated with vulnerabilities in the supply chain.

Likes 0	

Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	
Luminant wants to thank the Supply Chain SDT for their diligence in reviewing the previous comments and using those comments to appropriately craft the current proposed documents. Luminant also wants to encourage the SDT to review the comments submitted during this ballot period and consider changes to the standards, as appropriate, even if these standards are passed by the ballot body.	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response	
Scott Downey - Peak Reliability - 1	
Answer	
Document Name	
Comment	
Peak Reliability believes the proposals are a step in the right direction but as written do not provide the value intended.	
Likes 0	
Dislikes 0	

Response

Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance

Answer	
Document Name	

Comment

1) Make ‘vendor’ a defined term or provide GTB explanation for what is expected to be considered a vendor.

2) Guidelines and Technical Basis for CIP-013-3 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems can a reliable software update source be identified once?

3) Please provide implementation guidance on CIP-005 and CIP-010

4) Make ‘integrity’ a defined term or provide GTB explanation for what is expected for verifying integrity of software.

5) Please list practical ways to validate the integrity of software.

Likes 0	
Dislikes 0	

Response

Wesley Maurer - Lower Colorado River Authority - 5

Answer	
Document Name	

Comment

Make ‘vendor’ a defined term or provide GTB explanation for what is expected to be considered a vendor.

Guidelines and Technical Basis for CIP-013-3 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems can a reliable software update source be identified once?

Please provide implementation guidance on CIP-005 and CIP-010

Make ‘integrity’ a defined term or provide GTB explanation for what is expected for verifying integrity of software.

Please list practical ways to validate the integrity of software.

Likes 0	
Dislikes 0	

Response

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	
Document Name	
Comment	
GRE appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	
Document Name	
Comment	
No Cooent	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	
: The SDT doesn't address CIP Exceptional Circumstance (CEC) in any of the Supply Chain Standards. If an event does occur that creates a CEC, it could potentially cause an entity to not be able to monitor vendor remote access verification of software integrity and authenticity. In Order No. 829, it states, "new or modified 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." Does the drafting team have confidence that only having in scope medium and high BES Cyber Assets meets the directive for "industrial control system hardware, software, and services"?	

ACES recommends additional verbiage be written in the requirements to document what cyber assets that are not in scope for Supply Chain Management such as: Electronic Access Control and Monitoring Systems (EACMS), transient cyber assets, removable media and protected cyber assets (PCA).

Thank you for your time and consideration.

Likes 0	
Dislikes 0	

Response

Theresa Rakowsky - Puget Sound Energy, Inc. - 1

Answer	
Document Name	

Comment

PSE supports comments submitted by EEI.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion

Answer	
Document Name	

Comment

No comment

Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	

Response

Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	

Document Name	
Comment	
GTC appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. Therefore, the IRC suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IRC suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
1. Make 'vendor' a defined term or provide GTB explanation for what is expected to be considered a vendor.	

2. Guidelines and Technical Basis for CIP-013-3 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems, can a reliable software update source be identified once?

3. Please provide implementation guidance on CIP-005 and CIP-010.

4. Make 'integrity' a defimed term or provide GTB explanation for what is expected for verifying integrity of software.

5. Please list practical ways to validate the integrity of software.

Likes 0	
Dislikes 0	

Response

William Harris - Foundation for Resilient Societies - 8

Answer	
Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx

Comment

See combined comments of the Foundation for Resilioent Sociewties in the attached file.

Likes 0	
Dislikes 0	

Response

John Martinsen - Public Utility District No. 1 of Snohomish County - 4

Answer	
Document Name	

Comment

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.

Likes 0	
Dislikes 0	

Response

Long Duong - Public Utility District No. 1 of Snohomish County - 1

Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Franklin Lu - Snohomish County PUD No. 1 - 6	

Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments of the IRC and offers the following additional comment: The term “vendor” that is used repeatedly in the rationale boxes requires further clarification or revision. “A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.” Services cannot be manufactured, and the provision of services is already addressed through item (ii). ERCOT suggests the following revision: “A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems or components; (ii) *providers of information systems services*; (iii) product resellers; or (iv) system integrators.”	
Likes 0	
Dislikes 0	
Response	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	

Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
Regarding requirement R2, measure M2, suggest consider revising language to state "…demonstrate use of ***or compliance with*** *the supply chain cyber security risk management plan."*	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	
Document Name	
Comment	
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.	
Likes 0	
Dislikes 0	
Response	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	
Document Name	
Comment	

CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.

Likes 0	
Dislikes 0	

Response

Chad Bowman - Public Utility District No. 1 of Chelan County - 1

Answer	
Document Name	

Comment

CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.

Likes 0	
Dislikes 0	

Response

Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion

Answer	
Document Name	

Comment

Dominion recommends the following changes to the RSAWs:

- CIP-005-6, R2, Parts 2.4 and 2.5
  - Remove the word “all” from the “Compliance Assessment Approach sections.
- CIP-010-3, R1, Part 1.6
  - Remove the words “for each” from the “Compliance Assessment Approach section, rows 2 and 4.

- CIP-013-1, R1
    - Remove the word “controls”. The word “processes” is now in uses in the most current draft of CIP-013-1.

Likes 0	
Dislikes 0	

Response

Mick Neshem - Public Utility District No. 1 of Chelan County - 3

Answer	
Document Name	

Comment

CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.

Likes 0	
Dislikes 0	

Response

Patrick Hughes - National Electrical Manufacturers Association - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	NEMA Comments on NERC Supply Chain Risk Management 2017-06-12.pdf

Comment

On behalf of the National Electrical Manufacturers Association (NEMA)—a trade association and standards developing organization with nearly 350 member companies that manufacture a diverse set of products used in the generation, transmission, distribution, and end-use of electricity—and on behalf of the NEMA Grid Modernization Leadership Council and the NEMA Cybersecurity Committee, I wish to submit for your reference “CPSP 1-2015: Supply Chain Best Practices,” which describes industry best practices for manufacturers to follow regarding cybersecurity supply chain management.

“Supply Chain Best Practices” identifies guidelines that electrical equipment manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses or other exploits can be used can be used to negatively impact product operation. It addresses United States supply chain integrity through four phases of a product’s life cycle: manufacturing, delivery, operation, and end-of-life. The report (attached) is available for public download at: http://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx.

The National Electrical Manufacturers Association and its members understand that a secure supply chain is essential to a secure grid and that cybersecurity aspects should be built into, not bolted onto, manufacturers' products. They also understand that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among electric utility companies and the manufacturers of critical electric grid systems and components—both hardware and software. NEMA looks forward to working with and being a resource for NERC, utilities, and other interested stakeholders in addressing supply chain risks and concerns within the energy sector.

Should you have any questions, please contact Patrick Hughes, Senior Director of Government Relations and Strategic Initiatives, at 703-841-3205 or patrick.hughes@nema.org.

Respectfully,

Kyle Pitsor

Vice President, Government Relations

Likes 0	
Dislikes 0	

Response

Steven Sconce - EDF Renewable Energy - 5

Answer	
Document Name	

Comment

No comment.

Likes 0	
Dislikes 0	

Response

Louis Guidry - Louis Guidry On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 3, 1; Michelle Corley, Cleco Corporation, 6, 5, 3, 1; Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; Stephanie Huffman, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry

Answer	
Document Name	

Comment

The Guidance and Techincal Basis section is empty.

Likes 0	
Dislikes 0	

Response

Thomas Foltz - AEP - 5	
Answer	
Document Name	

Comment
AEP urges the SDT to consider FERC Order 706 paragraph 355 which requires a policy for each of the cyber security topical areas. CIP-003 R1 should require a policy for supply chain cyber security.

Likes 0	
Dislikes 0	

Response

Tyson Archie - Platte River Power Authority - 5	
Answer	
Document Name	

Comment
Platte River Power Authority also supports the comments submitted by the American Public Power Association (APPA)

Likes 0	
Dislikes 0	

Response

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	

Comment

CenterPoint Energy appreciates the Standard Drafting Team's thorough consideration of comments. Although some concerns with implementation remain, CenterPoint Energy believes that the revisions have made the draft Standard focused and risk-based. CenterPoint Energy also commends the coordination with the CIP Modifications team to place certain requirements appropriately in the body of the existing CIP Standards. Thank you for your efforts.	
Likes 0	
Dislikes 0	
Response	
Andrew Gallo - Austin Energy - 6	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Qu?bec Production - 5	
Answer	
Document Name	
Comment	

No comment

Likes 0	
Dislikes 0	

Response

Lona Calderon - Salt River Project - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF

Answer	
Document Name	

Comment

The American Council of Engineering Companies (ACEC) -the business association of the nation's engineering industry - wants to convey the industry's perspectives and concerns over the development of this new cyber security supply chain rule mandated by the Federal Energy Regulatory Commission (FERC).

ACEC members firms, numbering more than 5,000 and representing over 500,000 employees throughout the country, are engaged in a wide range of engineering work that propel the nation's economy, and enhance and safeguard America's quality of life. Council members are actively involved in every aspect of the energy marketplace. Supply chain cyber security is of growing concern to all our members.

ACEC is in agreement with most of the comments of the owners, operators, vendors and suppliers that have formally participated in this Standard development.

Likes 0	
Dislikes 0	

Response

Barry Lawson - National Rural Electric Cooperative Association - 4

Answer	
Document Name	

Comment

NRECA appreciates the work and efforts of the SDT.

Likes 0	
Dislikes 0	

Response

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI greatly appreciates the work of the SDT and NERC in reviewing and addressing stakeholder feedback from the first ballot. EEI supports the currently posted drafts and ask that the SDT look to our members' individual comments for further suggestions for improvement.

Likes 0	
Dislikes 0	

Response

David Rivera - New York Power Authority - 3

Answer	
Document Name	

Comment

None.

Likes 0	
Dislikes 0	

Response

Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF

Answer	
Document Name	

Comment
Please note that the NSRF has concerns with the Webinar and Guidance going outside of the scope of the proposed Requirements. All applicable entities will need to satisfy the Requirements once approved by FERC per FERC Order 693, setcion253. Regardless of what the Webinar or Guideline states.

Likes 0	
Dislikes 0	

Response

Chris Scanlon - Exelon - 1	
Answer	
Document Name	

Comment
None.

Likes 0	
Dislikes 0	

Response

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment
No comment

Likes 0	
Dislikes 0	

Response

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	
Document Name	

Comment

GSOC appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

Additional comments received from Seattle City Light

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments: *Note that for all comments (1-9) written in blue text come directly from APPA and/or LPPC comments. Any comments in black are City Light's.*

Seattle City Light continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

Seattle agrees with limiting the requirement to high and medium assets only.

R1: Seattle generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, might be included in the standard for these kinds of procurement activities. Alternatively, concerns about how different type of contracts—multi-party contracts, master agreements, evergreen agreements, piggyback contracts, long-term service agreements, etc, etc, etc—may or may not comply might be addressed by re-positioning CIP-013 as a performance-based Standard, with a focus on managing specific aspects of vendor security rather than particular contracting practices.

Our reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and (attempt to) achieve the protections identified in R1.2. It is immaterial how these protections are pursued. Focusing vendor security plans and audit approaches on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such we suggest that R1.2 be revised as follows:

1.2. *One or more process(es) for its newly procured BES Cyber Systems that address the following elements, as applicable:*

As explanation for the revisions, underlined words are added, and "newly" is intended to mean 'obtained after the implementation of CIP-013.' Also, the term "elements," as shown above, is added to more clearly align with the VSLs for this requirement.

At the same time guidance associated with the "Rationale for R1," "Rationale for R2," and the separate Implementation Guidance document should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no necessary function in vendor security plans and audit approaches. Contract terms might be used by an entity in their vendor security plans and/or as evidence of performance, but there should be no expectation by auditors or subtext in the Standard or Implementation Guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what contract terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately there should be no expectation that CIP-013 R1.2 protections be achieved through the contracting process. Consistent with performance-based standard principles the objective in CIP-013 and in entity vendor security plans should be on achieving each protection (as feasible), not on the means by which it is achieved (or attempted to be achieved).

In the absence of such changes, we request substantial additional clarification about how, without contract terms and contract negotiations being auditable, performance of R2 implementation will be audited and assessed. In particular for state and regional master agreements, piggyback contracts, evergreen agreements, and the like.

Looking to specific details of CIP-013 requirements, Seattle requests re-wording of R1 parts 1.2.1 and 1.2.4 to better understand what is expected. These parts appear to be duplicative. The endorsed Guidance does not adequately distinguish between the two parts. One interpretation is that part 1.2.1 is for products/services and that part 1.2.4 is for vulnerabilities in the product. It is not clear if these parts expect information sharing at the time of procurement or if information sharing will be on-going?

In R1 parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor, or incidents identified by the vendor. Seattle suggests changing "identified" in the phrase, to "acknowledged" or "confirmed" to ensure clarity.

Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.

Seattle believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that entities include their definition of "vendor" in their plan(s).

Seattle recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: Seattle agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

As discussed above, Seattle urges the significant additional guidance, preferably centered on performance-based principles, about expected compliance practices and how implementation will be audited. In particular for state and regional master agreements, piggyback contracts, evergreen agreements, and the like.

Finally, the Compliance and/or Implementation Guidance should make clear that, when evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

R3: Seattle agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, Seattle proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

The proposed CIP-005-6 uses the term, "vendor." The definition of vendor is not a NERC defined term. Seattle City Light believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that Entities include their definition of "vendor" in their plan(s).

Seattle agrees with R2 Part 2.4 but requests clarification of the term "determining."

Seattle generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective "is for entities to have the ability to rapidly disable active remote access sessions…" The Responsible Entity may not have the capability to disable access during an "active" remote access session. Seattle requests changing the language to "upon detected unauthorized activity."

Guideline & Technical Basis (GTB) for R2 should be included in this revision. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Please Include reference to FERC Order 829 for parts 2.4 and 2.5.

The SDT should consider adding a CIP Exceptional Circumstance clause to R2 parts 2.4 and 2.5

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light agrees this requirement belongs in CIP-010 R1. Seattle generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- Seattle recommends the Guidelines and Technical Basis section is updated to reflect current information.
  - The requirement states "For 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…," indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such

verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

  - Seattle also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third-party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed, in particular for R1.6.1 and R1.6.2. Additionally, Seattle requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While Seattle supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and minimize audit challenges.

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments: Seattle City Light agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. Among other things, the Order requests a risk-based approach. Application of Standard CIP-002 is an established, Commission-approved approach to categorize a utility's BES Cyber Systems into high, medium, and low risk classifications. Application of this established risk-based approach to cyber asset procurement for electric utilities is natural, appropriate, and consistent with the guiding CIP philosophy, stated in Section 6 of each CIP Standard, that each Standard "exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems."

Furthermore, Seattle believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and High requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach, as appropriate to the low BES risk presented by these entities.

Seattle believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items, beyond the benefit provided by additional controls. Existing controls inherent to CIP-003 and previous CIP Standards reduce the risk associated with Lows.

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. Seattle feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.

Seattle, in line with our recommendation to move CIP-013 to a performance-based standard as discussed in Question 1 above, also recommends deleting discussion of contracts and contract dates from implementation guidance, and focusing the guidance on BES Cyber Assets procured subsequent to the implementation date of the standard. If performance-based principles are not adopted, Seattle at least asks for clarity to change this General Consideration from:

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To:

Supply Chain Risk Management plan must be used by appropriate procurement processes that begin on or after the implementation date. (Also make corresponding change to the associated note in CIP-013 R2.)

Further, Seattle requests clarification on if/when existing contracts, master contracts, or long-term maintenance agreements that may be re-opened for renegotiation or later put in use (e.g., a state master contract negotiated prior to the CIP-013 implementation date but not actually used by a utility until after CIP-013 implementation date), come into the scope of CIP-013. Seattle notes that shifting to a performance-based Standard, focused on specific vendor protections and not the means that such protections are achieved (i.e., contracts) would minimize the explanations required about such matters.

The Implementation Plan does not handle unplanned changes such as newly identified IROLs or registration changes, etc, that may bring an entity suddenly into scope for CIP-013, CIP-005 R2.4-2.5, and/or CIP-010 R1.6. Seattle therefore requests that the Implementation Plan be modified to

address, in a reasonable way, how entities come into compliance if, due to changes, they newly meet applicability at some time after the effective date of the standards.

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

☐ Yes

☒ No

Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light agrees with the VRFs and VSLs for CIP-013. As discussed above under Question 1, Seattle requests that the term "elements" be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement.

For CIP-010, Seattle does not find that the VSL covers failures to implement the process. It therefore does not include all possible combinations of violation. Consequently, we request that there be an identified severity level for failure to implement and lower severity levels when a single aspect of the requirements is missing.

For CIP-005, Seattle believes that the VRFs and VSLs should be updated to reflect the same general structure used in CIP-010. The VSL for CIP-005 results in a "Severe" penalty if the entity did not have a method to determine and did not have a method to disable. Seattle would prefer a "High" VSL penalty if the entity has a process to determine but does not have a process to disable, and vice-versa if the entity did not have a process to determine but does have a process to disable.

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☐ Yes

☒ No

Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. Seattle is concerned about the possibilities that NERC and the Regions may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, Seattle would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard, including for CIP-005-6 R2.4 and R2.5 and for CIP-010-3 R1.6.

As discussed above, “vendor” is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005. Seattle believes the SDT should provide guidance regarding the use of the term “vendor.” If “vendor” is not defined by NERC, the Guidance should recommend that entities include their definition of “vendor” in their plan(s).

Neither of the bullets for R3 in the Implementation Guidance sufficiently explain compliance needs because both bullets only deal with plan review and not approval, both of which are necessary for compliance. Therefore, Seattle recommends changing:

”Below are some examples of approaches to comply with this requirement:“

to

“Below is an example of an approach to comply with the review requirement required by: “

In addition, we recommend deleting the following guidance language from the second main bullet, because it is beyond the Requirement and introduced activities that are not explicitly required:

“Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☒ Yes

☐ No

Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if that if, due to uncertainty, anticipated audit risk, an eventually established audit approach, or any other reason, Standard CIP-013 precludes or has a chilling effect on use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other publics with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually to replace pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, Seattle strongly urges that audit approach language for CIP-013 R2 be clarified in advance to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions, auditors, time, and chance.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. Seattle suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or

alternatively that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

9. Provide any additional comments for the SDT to consider, if desired.

Comments: None

THE FOUNDATION FOR RESILIENT SOCIETIES COMMENTS AS FOLLOWS *ON PROPOSED STANDARD*

2016-03, CYBER SUPPLY CHAIN RISK MANAGEMENT, CIP-005-6, CIP-010-3, AND CIP-013-1:

Filed with NERC June 15, 2017

1. These NERC/SDT attempts to produce a CIP standard for supply chain vulnerabilities fall short in an extreme threat environment. Adversaries' efforts against the electric grid and other civil infrastructure show disdain for U.S. defenses and deep commitment to using Information Operations (including cyber warfare) against the nation. The Bulk Electric System (BES) is a major target—this motivates development of strong capabilities for cyberattack. Adversaries understand full well the dependencies of social and national security institutions and all other critical infrastructures on electric power.

2. There is insufficient substance to the draft standard, other than the usual CIP generalized statements of planning, implementation, and periodic reviews that provide *pro forma* response to FERC Order No. 829. In its 9-1 vote to reject the first draft, the industry sent a clear message to NERC and FERC: the standard requirements are, at present, inadequately defined and therefore the feasibility of cost recovery is hard to judge.

3. Any sincere attempt at compliance with the draft standard requirements by responsible entities will incur high costs with uncertain benefit to the survivability of the BES. The Standard Drafting Team appears to minimize the complexity of the 2014 Russian penetrations of the U.S. BES, its sophisticated multi-layered, years-earlier penetration of vendor's control systems, phishing efforts, firmware modifications, and extensive use of IT vendors' vulnerabilities in operating, communications and networking, and database systems. The draft lacks good protective steps on these vulnerabilities and is therefore inadequate for mitigating risk--especially given the increasing nature of the Russian Havex and BlackEnergy threats evidenced in the follow-on attacks in the Ukraine Grid in 2015 and 2016. Note the recent revelation by ESET and DRAGOS of CRASH OVERIDE malware (associated with the 2016 Ukraine attack) with specific and flexible targeting of "low impact" industrial control systems (ICS). Note also the increasing threat from Distributed Denial of Service (DDoS) IoT and ransomware attacks. To expect several thousand utilities to individually and separately determine self-protective actions under the draft standard is unrealistic. Economies of scale in protection are needed.

4. Exempting "Low Impact" cyber systems leaves vulnerabilities. Also, as Resilient Societies has pointed out on FERC dockets, the exclusion from CIP Standards for all communications and networks between "Electronic Security Perimeters," together with direct internet connectivity to many so-called "low impact" cyber assets, leaves literally thousands of unsecured channels for malware implantation.

5. Stringent application whitelisting/blacklisting and selective third party certification steps, in conjunction with a national deterrence policy, are needed to enhance the minimal-protection from current CIP standards.

6. Ambiguities in standard requirements result in a lack of auditability, as noted by many other commenters.
7. In the short-term, a more practical NERC initiative could be to support a FERC rulemaking to require Bulk Electric System-jurisdictional entities to detect, report, mitigate and remove malware. State PUCs should likewise support a malware mitigation initiative for distribution utilities.

William R. Harris

Foundation for Resilient Societies, Inc.

Additional comments received from Independent Electric System Operator

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

☐ Yes

☒ No

Comments: The IESO agrees in principle with the proposed requirements and respectfully submit suggestions for purposes of clarity.

Requirement 1.2.1

We suggest the following wording change as the current wording suggests that the vendor has sufficient knowledge of the Responsible Entities' environment to know that a particular vulnerability does in fact pose a security risk to the Responsible Entity.

Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that *could* pose cyber security risk to the Responsible Entity;

Requirement 1.2.2

We suggest the following wording change as the current phrase "coordination of response" is not clear as to what is intended by "coordination".

Coordination of response *activities by the vendor and the Responsible Entity* to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

Requirement 1.2.3

We suggest the following wording change as the current wording suggests that the Vendor has sufficient knowledge of the Responsible Entity to determine whether or not an individual should no longer be granted access. The Responsible Entity is the only party to an agreement that has the ability to determine who should or should not have access.

Circumstances where vendors should notify the Responsible Entity that access requirements of the vendor or third party personnel has changed.

Requirement 1.2.4

We suggest the following wording change as the current wording is not clear as to which vulnerabilities are applicable.

Disclosure by vendors of known vulnerabilities *in the procured product or service;*

Requirement 1.2.6

We suggest the following wording change as the use of the phrase “Coordination of controls” is confusing.

Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments: The IESO agree with the new CIP-005-6 Requirement R2 Parts 2.4 and 2.5 however we note there is no corresponding “Guidance and Technical Basis” or “Rationale”

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

☐ Yes

☒ No

Comments: The IESO is concerned with two aspects of CIP-010-3 Requirement R1 Part 1.6:

1. The phrase “when the method to do so is available to the Responsible Entity from the software source” will be difficult to audit and difficult for the Responsible Entity to confirm as it is hard to prove a negative. The IESO suggest that verification of software source and integrity can take many different forms and is a sufficiently common practice that this phrase is not required. To take into consideration legacy software, the IESO suggest the wording be adjusted, to reflect FERC intentions that the requirements are forward looking, by replacing the phrase “and when the method to do so is available to the Responsible Entity from the software source” with “and, at a minimum, for the portion of the software that has changed:”

2. There appears to be inconsistency between the requirement and the Guidelines.

The requirement states “For 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”.

The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit.

Therefor the IESO suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IESO suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT’s removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☐ Yes

☐ No

Comments: As the IESO does not have any low impact BES Cyber Systems we abstain from answering Yes or No to this question. However, we suggest the rationale for not including Low Impact Bes Cyber Systems is not clear. We also suggest that small to medium sized Responsible Entities have the most to gain from CIP-013 as they have the fewest resources to mitigate risks from the supply chain.

While the IIESO does not have Low Impact Bes Cyber Systems we have multiple interfaces with our Market Participants that do have Low Impact BES Cyber Systems. This, in turn represents, risk to our BES Cyber Systems. As such we recommend that CIP-013-1 apply to Low Impact BES Cyber Systems to reduce the supply chain risk not only to the Low Impact BES Cyber Systems but to the IRC member organization’s BES Cyber Systems.

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments:

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments:

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☒ Yes

☐ No

Comments: Note: the following comment is the same as identified for question 3.

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☒ Yes

☐ No

Comments:

9. Provide any additional comments for the SDT to consider, if desired.

Comments:

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states "For 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".

The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit.

Therefor the IESO suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IESO suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.

Note: the following comment is the same as identified for question 2.

We note there is no corresponding “Guidance and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name:	2016-03 Cyber Security Supply Chain Risk Management | CIP-005-6, CIP-010-3, CIP-013-1
Comment Period Start Date:	5/2/2017
Comment Period End Date:	6/15/2017
Associated Ballots:	2016-03 Cyber Security Supply Chain Risk Management CIP-005-6 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-010-3 IN 1 ST 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 AB 2 ST

There were 101 sets of responses, including comments from approximately 220 different people from approximately 141 companies representing 10 of the Industry Segments as shown in the table on the following pages.

The Project 2016-03 Standards Drafting Team (SDT) appreciates the careful review and constructive feedback from stakeholders. The SDT made clarifying and non-substantive changes suggested by stakeholders to the proposed Reliability Standards as follows:

CIP-013-1

- Clarified wording in Requirement R1 Part 1.2.4 for consistency
- Revised examples of procurement processes listed in Requirement R1 rationale to include cooperative purchase agreements
- Clarified in Requirement R3 rationale that responsible entities are not required to renegotiate contracts when implementing updated plans
- Revised the Violation Severity Level (VSL) for Requirement R2 to describe four levels (Lower, Moderate, High, and Severe)

CIP-005-6

- Revised rationale to clarify that responsible entities do not need to implement remote access management processes if they do not allow remote access to applicable BES Cyber Systems, consistent with approved CIP-005-5
- Clarified in the rationale that the phrase *vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* used in the Requirement covers all remote access sessions with vendors.
- Revised VSL for Requirement R2 to include an additional level (High)

CIP-010-3

- Clarified in Requirement R1 Part 1.6 that responsible entities are required to perform software verifications **prior to** a change in baseline
- Revised the Measure for Part 1.6 to include evidence that could apply to automated update systems
- Added information to the Guidelines and Technical Basis section for Requirement R1

Implementation Plan

- Revised examples of procurement processes listed in General Considerations to include cooperative purchase agreements
- Adopted clearer wording for General Considerations section as recommended by commenters
- Added statement to affirm applicability to high and medium impact BES Cyber Systems only
- Included implementation provisions for planned and unplanned changes in categorization consistent with Version 5 CIP Standards implementation

Responses to all comments are provided in the following sections.
All comments submitted can be reviewed in their original format on the project page.

If you feel that your comment has been overlooked, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Director of Standards Development, Steve Noess (via email) or at (404) 446-9691.

Questions

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

9. Provide any additional comments for the SDT to consider, if desired.

The Industry Segments are:

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

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim	1,3,4,5,6	RF	FirstEnergy Corporation	Aaron Ghdooshim	FirstEnergy - FirstEnergy Corporation	4	RF
					Aubrey Short	FirstEnergy - FirstEnergy Corporation	1	RF
					Theresa Ciancio	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Ann Ivanc	FirstEnergy - FirstEnergy Solutions	6	RF
Southern Company - Southern Company Services, Inc.	Brandon Cain	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company - Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Southern Company - Alabama Power Company	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					William D. Shultz	Southern Company - Southern Company Generation	5	SERC
					Jennifer Sykes	Southern Company - Southern Company Generation and Energy Marketing	6	SERC
Luminant - Luminant Energy	Brenda Hampton	6		Luminant	Brenda Hampton	Luminant - Luminant Energy	6	Texas RE
					Stewart Rake	Luminant Mining Company LLC	7	Texas RE
					Alshare Hughes	Luminant - Luminant Generation Company LLC	5	Texas RE
Tennessee Valley Authority	Brian Millard	1,3,5,6	SERC	Tennessee Valley Authority	Scott, Howell D.	Tennessee Valley Authority	1	SERC
					Grant, Ian S.	Tennessee Valley Authority	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Thomas, M. Lee	Tennessee Valley Authority	5	SERC
					Parsons, Marjorie S.	Tennessee Valley Authority	6	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
SRC	David Francis	1,2	FRCC,MRO,NPCC, RF,SERC,SPP RE,Texas RE,WECC	SRC + SWG	Gregory Campoli	New York Independent System Operator	2	NPCC
					Mark Holman	PJM Interconnection, L.L.C.	2	RF
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	SPP RE
					Terry BIlke	Midcontinent ISO, Inc.	2	RF
					Elizabeth Axson	Electric Reliability Council of Texas, Inc.	2,3	Texas RE
					Ben Li	IESO	1	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Drew Bonser	SWG	NA - Not Applicable	NA - Not Applicable
					Darrem Lamb	CAISO	2	WECC
Seattle City Light	Ginette Lacasse	1,3,4,5,6	WECC	Seattle City Light Ballot Body	Pawel Krupa	Seattle City Light	1	WECC
					Hao Li	Seattle City Light	4	WECC
					Bud (Charles) Freeman	Seattle City Light	6	WECC
					Mike Haynes	Seattle City Light	5	WECC
					Michael Watkins	Seattle City Light	1,4	WECC
					Faz Kasraie	Seattle City Light	5	WECC
					John Clark	Seattle City Light	6	WECC
					Tuan Tran	Seattle City Light	3	WECC
					Laurrie Hammack	Seattle City Light	3	WECC
Entergy	Julie Hall	6		Entergy/NERC Compliance	Oliver Burke	Entergy - Entergy Services, Inc.	1	SERC
					Jaclyn Massey	Entergy - Entergy Services, Inc.	5	SERC
Associated Electric	Mark Riley	1		AECI & Member G&Ts	Mark Riley	Associated Electric Cooperative, Inc.	1	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Cooperative, Inc.					Brian Ackermann	Associated Electric Cooperative, Inc.	6	SERC
					Brad Haralson	Associated Electric Cooperative, Inc.	5	SERC
					Todd Bennett	Associated Electric Cooperative, Inc.	3	SERC
					Michael Bax	Central Electric Power Cooperative (Missouri)	1	SERC
					Adam Weber	Central Electric Power Cooperative (Missouri)	3	SERC
					Ted Hilmes	KAMO Electric Cooperative	3	SERC
					Walter Kenyon	KAMO Electric Cooperative	1	SERC
					Stephen Pogue	M and A Electric Power Cooperative	3	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					William Price	M and A Electric Power Cooperative	1	SERC
					Mark Ramsey	N.W. Electric Power Cooperative, Inc.	1	SERC
					Kevin White	Northeast Missouri Electric Power Cooperative	1	SERC
					Skyler Wiegmann	Northeast Missouri Electric Power Cooperative	3	SERC
					John Stickley	NW Electric Power Cooperative, Inc.	3	SERC
					Jeff Neas	Sho-Me Power Electric Cooperative	3	SERC
					Peter Dawson	Sho-Me Power Electric Cooperative	1	SERC
	Michael Shaw	6			Teresa Cantwell	LCRA	1	Texas RE

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Lower Colorado River Authority				LCRA Compliance	Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
BC Hydro and Power Authority	Patricia Robertson	1		BC Hydro	Patricia Robertson	BC Hydro and Power Authority	1	WECC
					Venkataramakrishnan Vinnakota	BC Hydro and Power Authority	2	WECC
					Pat G. Harrington	BC Hydro and Power Authority	3	WECC
					Clement Ma	BC Hydro and Power Authority	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	RSC no Dominion	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC
					Bruce Metruck	New York Power Authority	6	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Alan Adamson	New York State Reliability Council	7	NPCC
					Edward Bedder	Orange & Rockland Utilities	1	NPCC
					David Burke	Orange & Rockland Utilities	3	NPCC
					Michele Tondalo	UI	1	NPCC
					Sylvain Clermont	Hydro Quebec	1	NPCC
					Si Truc Phan	Hydro Quebec	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Laura Mcleod	NB Power	1	NPCC
					Michael Forte	Con Edison	1	NPCC
					Kelly Silver	Con Edison	3	NPCC
					Peter Yost	Con Edison	4	NPCC
					Brian O'Boyle	Con Edison	5	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
					David Ramkalawan	Ontario Power Generation Inc.	5	NPCC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Quintin Lee	Eversource Energy	1	NPCC
					Kathleen Goodman	ISO-NE	2	NPCC
					Greg Campoli	NYISO	2	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	6	NPCC
Midwest Reliability Organization	Russel Mountjoy	10		MRO NSRF	Joseph DePoorter	Madison Gas & Electric	3,4,5,6	MRO
					Larry Heckert	Alliant Energy	4	MRO
					Amy Casucelli	Xcel Energy	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jodi Jensen	Western Area Power Administratino	1,6	MRO
					Kayleigh Wilkerson	Lincoln Electric System	1,3,5,6	MRO
					Mahmood Safi	Omaha Public Power District	1,3,5,6	MRO
					Brad Parret	Minnesota Power	1,5	MRO

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Terry Harbour	MidAmerican Energy Company	1,3	MRO
					Tom Breene	Wisconsin Public Service	3,5,6	MRO
					Jeremy Volls	Basin Electric Power Coop	1	MRO
					Kevin Lyons	Central Iowa Power Cooperative	1	MRO
					Mike Morrow	Midcontinent Independent System Operator	2	MRO
Scott Miller	Scott Miller		SERC	MEAG Power	Roger Brand	MEAG Power	3	SERC
					David Weekley	MEAG Power	1	SERC
					Steven Grego	MEAG Power	5	SERC
Dominion - Dominion Resources, Inc.	Sean Bodkin	6		Dominion	Connie Lowe	Dominion - Dominion Resources, Inc.	3	NA - Not Applicable
					Lou Oberski	Dominion - Dominion Resources, Inc.	5	NA - Not Applicable
					Larry Nash	Dominion - Dominion Virginia Power	1	NA - Not Applicable

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
Southwest Power Pool, Inc. (RTO)	Shannon Mickens	2	SPP RE	SPP Standards Review Group	Shannon Mickens	Southwest Power Pool Inc.	2	SPP RE
					Deborah McEndafffer	Midwest Energy, Inc	NA - Not Applicable	NA - Not Applicable
					Robert Gray	Board of Public Utilities (BPU) Kansas City, Kansas	3	SPP RE
					Louis Guidry	Cleco	1,3,5,6	SPP RE
					Megan Wagner	Westar Energy	6	SPP RE
PPL - Louisville Gas and Electric Co.	Shelby Wade	1,3,5,6	RF,SERC	PPL NERC Registered Affiliates	Charlie Freibert	LG&E and KU Energy, LLC	3	SERC
					Brenda Truhe	PPL Electric Utilities Corporation	1	RF
					Dan Wilson	LG&E and KU Energy, LLC	5	SERC
					Linn Oelker	LG&E and KU Energy, LLC	6	SERC
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE
ACES Power Marketing	Warren Cross	1,3,4,5	MRO,RF,SERC,SPP RE,Texas RE,WECC	ACES Standards Collaborators	Arizona Electric Power Cooperative, Inc.	AEPC	1	WECC
					Hoosier Energy Rural Electric Cooperative, Inc.	HE	1	RF
					Sunflower Electric Power Corporation	SEPC	1	SPP RE
					Rayburn Country Electric Cooperative	RCEC	3	SPP RE
					Old Dominion Electric Cooperative	ODEC	3,4	SERC
					Brazos Electric Power Cooperative, Inc.	BRAZOS	1,5	Texas RE

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46). The SDT believes it is appropriate to allow entities to have flexibility in determining whether the CIP Senior Manager or delegate should review and approve the plan. CIP-003-6 provides for policy review by CIP Senior Manager only.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	No

Document Name	
Comment	
Recommend removing those items covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy." The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely	

upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	No
Document Name	
Comment	
GRE supports the NRECA comments. In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.

Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	

Comments:

Concerned that the R1 guidance provides details which are beyond the scope of R1

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Recommend removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

{C}1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

-

- R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided examples of processes related to Part 1.2.1 through 1.2.6 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance. Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.

Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	No
Document Name	
Comment	

Texas RE notes that the proposed standard is not responsive to the FERC directive. FERC Order No. 829 P. 59 specifically states "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." The Note in Requirement R2, however, states: "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." Texas RE agrees that it is unreasonable to hold a registered entity accountable for a vendor's adherence to (or lack of adherence to) a contract. Texas RE agrees as the standard drafting team (SDT) claims obtaining specific controls in the negotiated contract may not be feasible at all times but Texas RE believes this is *best practice*. In fact, in most cases contracts for these types of systems typically include security provisions and set similar expectations as described in the standard. The proposed standards would prohibit the compliance monitor from verifying the registered entity implemented part 1.1 and sub-parts 1.2.1 through 1.2.7. Moreover, this verification is to ensure that the registered entities' plans are consistent with the contract's expectations and obligations of the parties.

Admittedly, there will be circumstances in which a contracts may not be consistent or silent as it pertains to the responsible entity's security management plans (e.g. existing contacts or contracts in which the responsible entity was unable to negotiate the appropriate terms into the contract.) In those circumstances, other evidence should be provided demonstrating that the responsible entity has processes to ensure the vendor is expected/obligated to act consistently with the responsible entity's cyber security risk management

plans as it relates to the vendor's products or services. Therefore, the contracts should remain in scope as to demonstrate the mapping of expectations from the plan to the contract as far as vendor interactions for those specific items included in the standard and to advance best practices leading to a more reliable BES.

Additionally, Texas RE has the following concerns:

- In the current CIP-013-1 version, the SDT elected to restrict the scope of the Supply Chain process to Medium and High Impact Bulk Electric System (BES) Cyber Systems, as well as exclude Physical Access Controls (PACS), Electronic Access Control and Monitoring Systems (EACMS), and Protected Cyber Assets (PCAs) from the scope of the Standard. In doing so, the SDT appeared to rely on a number of commenters that suggested that FERC Order No. 829, P. 59 excluded these types of devices. Specifically, these commenters pointed to the following language in the FERC Order: "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." FERC Order No. 829, P. 59. Accordingly, it appears that the SDT has concluded that PACS, EACMS, and PCAs collectively do not fall within the scope of "industrial control system hardware" or "computing and networking services associated with bulk electric system operations."

  Texas RE is concerned PACS, EACMS, and PCAs *do* fall within the scope of "industrial control system hardware" and "computing and networking services associated with bulk electric system operations" as those terms are used in FERC Order No. 829. PACS, EACMS, and PCAs are foundational equipment within a network's architecture. Moreover, these devices are vendor supported and exposed to the precise vulnerabilities identified in FERC's supply chain directive. Given these facts, Texas RE does not believe there is either a basis in FERC Order No. 829 or, more importantly, a reliability-based rationale for excluding them from the scope of CIP-013-1.

- Page 7, Part 1.1: While FERC Order No. 829 specifically uses the term "hardware", Texas RE notes the word "hardware" is not used in the standard language. Texas RE recommends replacing the word equipment with the term hardware in order to be consistent with the FERC Order.

- Page 8, Section 1.2.6: Texas RE recommends the SDT define or provide examples of the term "*system-to-system remote access*" as this is a broad term which can be interpreted in many different ways.

Likes	0	

Dislikes 0	

Response. Thank you for your comment. The SDT believes proposed CIP-013-1 meets the reliability objectives contained in the project SAR and Order No. 829. The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP or vendor negotiations. Evidence could include RFPs or other procurement correspondence that demonstrate the responsible entity's cyber security risk management concepts and controls. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21). The note in Requirement R2 excludes contracts because the responsible entity may not be able to obtain all security provisions in Parts 1.2.1 – 1.2.6 with all vendors since the requirements cannot 'directly impose obligations on suppliers, vendors, or other entities".

The SDT believes that requiring entities to implement supply chain cyber security risk management plans for BES Cyber Systems provides the intended reliability benefit, which applies to "industrial control system hardware, software, and services associated with bulk electric system operations" as specified in Order No. 829 (P. 43). The SDT believes entities should have flexibility to determine supply chain cyber security risk management controls for other cyber assets, including EACMS, PACS, and PCAs. The SDT believes this is an appropriate risk-based approach that allows entities to focus resources where they provide the most reliability benefit. Although EACMS, PACS, and PCA do not fall within the scope of the proposed CIP-013-1 requirements, an entity may decide to use some of the supply chain cyber security risk management controls, processes, and procedures in planning and procuring for these assets as are used for applicable high and medium impact BES Cyber System.

The SDT does not believe changing 'equipment' to 'hardware' in the proposed standard will provide additional clarity.

Requirement R1 Part 1.6 addresses controls for all remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45).

Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	No

Document Name	
Comment	
AECI supports NRECA's comments provided below: In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to	

procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.
Jason Snodgrass - Georgia Transmission Corporation - 1

Answer	No
Document Name	

Comment
GTC supports NRECA comments: In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Sytems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx
Comment	
The following comment covers several of the questions in one comment, submitted by the Foundation for Resilient Societies, Nashua, NH. (Comment at end of document)	
Likes 0	
Dislikes 0	
Response	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No

Document Name	
Comment	
ERCOT joins the comments of the IRC with the exception of the comment on Requirement R1, Part 1.1.	
Likes 0	
Dislikes 0	
Response	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	

Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons: • Is not performance based and therefore not auditable	

- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the

assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be

used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved. The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No

Document Name	
Comment	

In the Response to Comments the SDT asserts “Identifying and assessing cyber security risks in BES Cyber System planning. The SDT revised CIP-013-1 Requirement R1 Part 1.1 to “specify risks that Responsible Entities shall consider in planning for procurement of BES Cyber Systems“. Previously, commenters indicated that “the scope of cyber security risks being addressed in R1 is unclear**”**. The SDT removed unnecessary and unclear wording from Requirement R1s main requirement and revised Requirement R1 Part 1.1 to clarify the supply chain cyber security risks that must be addressed by the Responsible Entity in planning for the procurement of BES Cyber Systems.”

This change does not clearly identify the risks as previously noted by commenters.

Dominion recommends the following language change for CIP-013-1, R1 Part 1.1:

“Include one or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess, if applicable, the cyber security risk(s) of (i) procuring and installing vendor equipment and software; (ii) network architecture security; and (iii) transitions between vendor”

Dominion also recommends the following proposed language change for CIP-013-1 R1 Part 1.2:

“One or more process(es) used during procurement of BES Cyber Systems that address the following, as applicable:”

R3 needs to contain the caveat found in R2 that “[Revision] of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders).”

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes the suggested addition of network architecture security to Part 1.1 is potentially unclear and could have a variety of interpretations by responsible entities. The SDT does not support the suggested change.

The SDT does not believe the suggested change from *in* to *during* for Part 1.2 provides additional clarity. Requirement R3 specifies that entities must review and obtain CIP Senior Manager approval of its plan. The SDT does not believe the note about implementation is appropriate for R3. The note in R2 applies to implementation of the entity's plan and is not limited to the initial plan only. If an entity revises its plan at a later date and implements the revised plan, it is not required to renegotiate or abrogate existing contracts as indicated by the note in R2.

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	

Comments: Chelan PUD appreciates the efforts of the drafting team to revise CIP-013 in response to comments and recommendations provided previously. Although there are significant improvements in this version of the Draft Standard, CHPD believes that the Standard should not be approved for the following reasons:

- Is not performance based and therefore not auditable
- Creates risk for the responsible entities due to lack of auditability
- Likely to be costly to vendors due to having to respond to various entity contract requests

CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013. However; the note in R2 should be maintained that states:

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.

CHPD's reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such CHPD asks that R1.2 be revised as follows:

1.2. *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Note also that CHPD asks that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. Ultimately, there should be no expectation that the protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has revised the CIP-013-1 Rationale and the Implementation Plan to address commenter concerns with some types of contracts including multi-party contracts and master agreements. The SDT believes proposed CIP-013-1 provides entities with the necessary flexibility to develop its plan such that it will cover the procurement actions used by the responsible entity. The SDT does not agree with removing procurement-related objectives from the proposed standard, or removing the examples of procurement processes from the Implementation Guidance, as several FERC directives in Order No. 829 are directly related to procurement. The SDT has revised the VSL for Requirement R1 to remove the word *elements.* Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT agrees that entities may be using other activities in other phases of the life cycle to also mitigate cyber security risks, and that some of these may be covered by other Reliability Standards.	
Shawn Abrams - Santee Cooper - 1	
Answer	No
Document Name	
Comment	
The intent and purpose of CIP-013 is very dependent upon the Implementation Guidance document. We appreciate the hard work of the SDT to provide this document to industry and it has valuable information. A concern is that auditors can only audit to the requirements within the standard so some of the comments are based on needing more clarification within the standard itself. Language should be included in the standard (not just in the Rationale) that allows for inclusion of a clause in a procurement agreement stating that CIP-013 compliance must be met by the supplier unless it is either not offered or would significantly increase the cost of the agreement. (See CIP-013-1, Section B, Rationale for Requirement R1). This language in a procurement agreement, along with the supplier's stipulation that this compliance is either unavailable or will increase costs should constitute proof that CIP-013 compliance was considered by the Registered Entity but waived due to the supplier's inability to accommodate the requirement in a reasonable manner.	

The standard should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a supply chain cyber security risk management plan or plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Santee Cooper is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

This standard will create the need for entities to have an inventory tracking mechanism of products that are purchased under the supply chain risk management plan. For example, switches could be purchased for use in an IT department, not under the supply chain cyber security risk management plan, and this would preclude it from being used in a BES Cyber System. A CIP Exceptional circumstance or something similar should be added to the standard to allow an entity to use a piece of equipment not procured under the supply chain cyber security risk management plan rather than risk reliability of the BES.

Please add some wording to the requirement in the standard to address how far up the supply chain the plan applies to. If a laptop is purchased from a vendor is there an expectation that the cyber security risk management plan stop with that vendor or is there an expectation that the associated parts of the laptop fall under the plan? It's currently included in the rationale language but the rationale language cannot be audited.

What happens when a vendor is bought out by another vendor? Are you compliant until you have to negotiate a contract with the new vendor?

In R1 Parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing "identified to "acknowledged" or "confirmed."

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The proposed CIP-013-1 requirements provide entities with flexibility to develop and implement an entity-specific cyber security supply chain risk management plan. The ERO Enterprise-endorsed Implementation Guidance provides examples of approaches to be compliant with the standard. As stated in NERC's approved Compliance Guidance Policy, "Registered entities can rely upon [the examples] and be reasonably assured that compliance requirements will be met."

Proposed CIP-013-1 does not preclude an entity from including a clause in a procurement agreement stating that CIP-013 compliance must be met by the supplier as suggested by the commenter. However, the SDT does not agree that this should be required by CIP-013 because it could negatively impact the procurement process for responsible entities. Furthermore, the SDT notes that the standard is not intended to impose obligations directly on the vendor. (P. 36)

The proposed requirements provide flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples. Some situations, such as when contracts are negotiated on behalf of the responsible entity, could be met by providing input to parties negotiating on behalf of the responsible entity.

Proposed CIP-013-1 address an entity's obligations to mitigate cyber security risks in planning and procuring high and medium impact BES Cyber Systems. An entity's inventory management, operating actions and management decisions to address emergency circumstances are not in scope of the standard. The SDT does not believe an exception such as CIP Exceptional Circumstances is needed to address equipment use. An entity could include provisions in its plan regarding procurement of products and services in emergency situations.

Procurement processes specified in Part 1.2 address various vendor-related cyber security topics. As noted in the Rationale section, the term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. The rationale section, including vendor description, becomes part of the guidelines section of the standard following board adoption. An entity can provide additional clarification of vendor relationships in its plan.

CIP-013 does not require an entity to renegotiate a contract when a vendor is bought by another vendor. However, if the entity negotiates a new contract after the effective date of CIP-013, that procurement process would fall under CIP-013.

Implementation Guidance provides examples of processes to address Parts 1.2.1 and 1.2.2 that provide additional clarity. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
Recommend modifying CIP-007 and CIP-010 to include the proposed risk management elements proposed in CIP-013, or take the corresponding elements out of CIP-007 and CIP-010 to make CIP-013 more than just having a plan. There are no quantifiable measures in CIP-013 that really justify it as a stand-alone standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Proposed CIP-013-1 contains risk-based requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The standard addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems. The SDT does not believe additional clarity or efficiencies will be gained by introducing new requirements for BES Cyber System planning and procurement into CIP-007 or CIP-010.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	

Even though ReliabilityFirst believes the CIP-013-1 draft standard address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 and is a positive step in addressing cyber supply chain management, ReliabilityFirst Abstains mainly due to Requirement R1 missing Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following specific comments for consideration.

1. Requirement R1

    i. Even though Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs) were not specifically called out specifically in FERC Order 829, ReliabilityFirst believes the SDT needs to examine the possible risk of not including EACMS, PACS and PCA as part of Requirement R1 and go beyond what was stated in FERC Order 829. EACMs and PACS are critical cyber assets that control access and monitoring into the entities' ESPs and PSPs and should follow the Supply Chain standard/requirements as do the High and Medium Impact Cyber Systems. As for the PCAs, if they are compromised due to a vulnerability in the vendors supplied hardware or software, they can possibly affect high and medium impact BES Cyber Systems. ReliabilityFirst offers the following modifications for consideration:

        a. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber System and, [if applicable, associated Electronic Access Control and Monitoring (EACM), Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA)]. The plan(s) shall include:

Likes 0	
Dislikes 0	

Response. The SDT believes that requiring entities to implement supply chain cyber security risk management plans for BES Cyber Systems provides the intended reliability benefit, which applies to "industrial control system hardware, software, and services associated with bulk electric system operations" as specified in Order No. 829 (P. 43). The SDT believes entities should have flexibility to determine supply chain cyber security risk management controls for other cyber assets, including EACMS, PACS, and PCAs. The SDT believes this is an appropriate risk-based approach that allows entities to focus resources where they provide the most reliability benefit. Although EACMS, PACS, and PCA do not fall within the scope of the proposed CIP-013-1 requirements, an entity may decide to use some of the supply chain

cyber security risk management controls, processes, and procedures in planning and procuring for these assets as are used for applicable high and medium impact BES Cyber System.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	

- BC Hydro appreciates the direction of the revisions ie to remove enforcement actions against responsible entities that have limited ability to influence vendors. However, BC Hydro still believes some aspects of R1 will be difficult to manage / enforce, especially given the breadth of vendors many responsible entities have associated with their BCAs. Not all vendors are going to be able to accommodate the asks of the requirement.
- "Notification by the vendor…" suggests the vendor is expected to reach out to the responsible entity, and communication / transparency is endorsed through potential inclusion of terms in RFP's / contracts. This relies on the vendor honesty / transparency and there is no way to verify their attestations. The requirement focuses on entities reviewing vendor processes which may have limited impact on reliability.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes responsible entities can meet the requirements of Part 1.2 and has provided some examples of ways to do so in the Implementation Guidance. The SDT agrees that responsible entities may not have the ability to obtain each of its desired cyber security controls in its contract with each of its vendors. The objective is to address the topics in Part 1.2 in the procurement process, with recognition that the actual terms and conditions of a contract are not in scope.

The SDT believes that engaging vendors to obtain notifications of relevant vulnerability and security issues can benefit reliability. For example, negotiations with vendors could lead to establishing designated points of contact for communicating issues. Responsible entities have flexibility to include entity-specific proposed terms and conditions in its plan.

Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
R1 states that each RE must have a plan with one or more processes that address ....as applicable. Applicability is in the eye-of-beholder, however the requirement does not specifically say as identified by the Responsibility Entity, which auditors may take as a deliberate act not to include, interpreting that it is not up to the Responsibilty Entity to determin which are applicable.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. In Part 1.2, 'as applicable' provides for situations where some of the topics do not apply to a given procurement action. For example, not all vendors will require remote access and therefore Part 1.2.3 and/or Part 1.2.6 do not apply.	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	No
Document Name	
Comment	
The clarification that we don't have and would like from NERC/WECC is the intent of the following statement in CIP-013 R1.2.5 ***"Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System".*** There is no Guidelines and technical basis at the end of the standard for this	

This has a very large implication as this says all software provided by a vendor has to perform an integrity and authenticity verification. This could implicate a dedicated channel from the vendor validating through software certificates which would imply entities forcing software vendors to provide this mechanism, which the likelihood of meeting this for MS, Symantec, (non-control system software) is slim. MD5 checksums can not validate the integrity of the software as this hashing mechanism was broken in 2005 (although a lot of software vendors still use it).	
Likes 0	
Dislikes 0	
Response. The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its procurement processes (such as in Requests for Proposal, contract negotiations, or other procurement processes). Part 1.2.5 does not obligate the responsible entity to obtain, or the vendor to provide, the means for performing software verification. 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 terms and conditions ultimately negotiated by the parties and included in a contract. As a result, actual contract terms are not in scope for CIP-013.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation recommends the proposed standard differentiate between contractual and non-contractual purchases, such as commercial off-the-shelf (COTS) products or other purchases made without using a contract vehicle (e.g., credit card purchases or using repurposed equipment).	
Likes 0	

Dislikes 0	
Response. The proposed requirement provides flexibility for entities to distinguish cyber security risk management processes for various types of procurement activities in its plan. The SDT does not believe the standard should establish prescriptive requirements to differentiate. The SDT considers COTS procurements as a potential type of procurement to be addressed in the enity's plan.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	

Requirement R1.

Oncor agrees with the concept; however, Oncor believes the language for R1.1 should be revised as follows, *"(i) Responsible Entity procures and installs vendor equipment and software"*; and *"(ii) Responsible Entity transitions from one vendor(s) product or service to another vendor(s) product or service".*

For Requirement 1.2.1., the current wording suggests that the vendor has sufficient knowledge of Oncor's environment to know that a particular vulnerability does in fact pose a security risk to Oncor. We offer a recommendation on the language, *"Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that could pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.2. The current phrase "coordination of response" is not clear as to what is intended by "coordination". We offer a recommendation on the language, *"Coordination of response activities by the vendor and the Responsible Entity to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.3. The current wording suggests that the vendor has sufficient knowledge of Oncor to determine whether or not an individual should no longer be granted access. Oncor is the only party to an agreement that has the ability to determine who should or

should not have access. We offer a recommendation on the language, *"Circumstances where vendors should notify the Responsible Entity that access requirements of the vendor or third party personnel has changed, based on CIP-004, R5."*

Requirement 1.2.4. The current wording is not clear as to which vulnerabilities are applicable. We offer a recommendation on the language, *"Disclosure by vendors of known vulnerabilities in the procured product or service that follows a responsible disclosure process";* Guidance should also be added to reference US-CERT, NIST, or other industry sources.

Requirement 1.2.6. Oncor suggests the following wording change as the use of the phrase "Coordination of controls" is confusing. We offer a recommendation on the language, *"Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)."*

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT does not believe the suggested wording for Part 1.1 provides additional clarity.

The SDT intends for the Parts 1.2.1 – 1.2.6 to list topics that must be addressed in the responsible entity's procurement processes, and has avoided more prescriptive wording. Responsible entities may provide entity-specific details and clarifications in their supply chain cyber security risk management plans.

Andrew Meyers - Bonneville Power Administration - 6	
Answer	No
Document Name	
Comment	

BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not

"plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46). The SDT believes it is appropriate to allow entity's flexibility in determining whether the CIP Senior Manager or delegate should review and approve the plan. CIP-003-6 provides for policy review by CIP Senior Manager only.	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	No
Document Name	
Comment	
In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the	

term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	
Requirements R1 and R2 essentially shift the burden for ensuring that BES Cyber System hardware and software vendors, resellers, and integrators follow sound security management practices onto individual Responsible Entities, which N&ST considers both unfair and unreasonable, for small entities in particular. The just-endorsed (by NERC) CIP-013 Implementation Guidance document suggests an	

entity could address R1.1's requirement to "identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services" by means of a series of interactions with prospective vendors that comprise, for all intents and purposes, a risk assessment of the vendor, conducted by the entity. What recourse would a small entity have if a prospective supplier, perhaps the only one available, declined to cooperate with such an in-depth examination of its internal processes? R2, which requires the implementation of the entity's R1 plan(s), acknowledges a vendor may be disinclined to agree to contractual obligations to support one or more specific elements of an entity's R1 risk management plan. However, it contains no language that acknowledges this could make it difficult, if not impossible, for the entity to fully implement its R1 plan. N&ST believes this creates significant compliance risks for entities that may have few if any other options in some procurement situations. N&ST therefore recommends the addition of language similar to existing technical feasibility language in CIP-002 through CIP-011.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.3 (revocation of vendor remote access privileges) in its CIP-004 Access Management and/or Access Revocation documentation.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.6 (vendor remote access) in its CIP-005 ESP and Interactive Remote Access documentation.

N&ST recommends that R2 be modified to state that a Responsible Entity has the option of describing its implementation of R1 Part 1.2.5 (vendor software authenticity and integrity) in its CIP-010 Configuration Change Management documentation.

Initial CIP Senior Manager or delegate approval of risk management plan(s) should be added to R1. N&ST notes the initial implementation of R3 specified in the draft Implementation Plan is on or before the Effective Date. If that language is retained, there will be no need to add CIP Sr Manager or delegate approval to R1.

CIP-013 R2 and/or the Implementation Plan should contain "trigger" language for R2 that clarifies an entity must implement its R1 risk management plan(s) for new procurement contracts signed on or after the Effective Date of CIP-013. Entities with no new procurement contracts or no new in-progress procurements on the Effective Date should not be expected to be able to demonstrate compliance with R2 at that time.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT's approach with CIP-013-1 is consistent with Order No. 829, which directed NERC to develop requirements for NERC entities and to not impose obligations directly on vendors. The requirements provide responsible entities with flexibility to use tailored planning and procurement processes and do not obligate or hold the responsible entity accountable for vendor cooperation. The SDT believes the responsible entity can implement procurement processes as required by Part 1.2 without need for compliance exception because of the flexibility that is inherent in CIP-013. Examples of procurement processes are contained in the Implementation Guidance. Proposed CIP-013-1 Requirement R2 does not preclude the responsible entity from using the responsible entity's documentation related to other CIP standards. However, the documentation must demonstrate use of the responsible entity's supply chain cyber security risk management plan in procuring BES Cyber Systems. Proposed CIP-013-1 addresses initial approval of the responsible entity's plan through the Implementation Plan. The Implementation Plan specifies when an entity must begin using its plan, and has been revised for clarity (see Implementation Plan section). The SDT agrees that entities should not be expected to demonstrate compliance with Requirement R2 if the entity has not initiated procurement processes when the requirement is effective.

Don Schmit - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
NPPD supports the comments submitted by the MRO NSRF for CIP-013. In addition: NPPD is concerned that this Standard is not sufficiently represented to be auditable. First, the Standard is not performance based, which leads to auditor discretion, which leads to inconsistency among the Regional Entities across the NERC footprint. Second, the Implementation Guidance document has words that protect the entities from interpretation risk, however are not part of the Standard; which leaves the auditor to determine the intent of the drafting team. This is true in the rationale section for R1 which has wording which would minimize interpretation risk to entities, however are not reflected in the Standard. The Rationale states that the supplier must	

meet CIP-013 unless it is either not offered by the supplier or would significantly increase the cost of the agreement. This needs to be included in the Standard or as a footnote in the Standard. This would be very important to clarity in audit practices. In addition, the Standard should specifically state that as long as evidence demonstrates that all items expressly identified in R1 are contained in the "plan" and are implemented via R2 that entities shall not be out of compliance (there should be no findings for opinion on intent or security).

As with other recently produced CIP Standards, this Standard is being "rushed" to satisfy a FERC directive and without concise and clear wording, implementation considerations of all impacted parties, and the means for auditors to audit to a performance based Standard and understood audit practices. An extended comment/balloting period should be requested of NERC/FERC in order to produce an auditable Standard.

Other comments:

There are no parameters for Standard applicability. If a piece of equipment is purchased and the vendor and entity meet the Standard, do subsequent purchases of associated parts relative to the equipment or replacement parts of the equipment from other vendors need to also meet the Standard?

R1 Parts 1.2.1 and 1.2.2 "vendor-identified incident" is not clear. This needs to have clarity added in the Standard. In addition "identified" should be changed to "confirmed".

CIP-013 R1 parts 1.2.5 and 1.2.6 are covered in CIP-005 and CIP-010. CIP-013 parts 1.2.5 and 1.2.6 should be removed to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

The responsible entity's supply chain cyber security risk management plan applies to high and medium impact BES Cyber Systems and must include procurement processes as specified in Part 1.2. The responsible entity is required to implement its plan, per Requirement R2. Any procurements of BES Cyber Systems including replacement of BES Cyber Systems, falls in scope of the entity's plan.

Implementation Guidance provides examples of processes to address Parts 1.2.1 and 1.2.2 that provide additional clarity. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	No
Document Name	
Comment	
GSOC supports NRECA's Comments of:	

In R1, NRECA recommends that the SDT reiterate "high and medium impact" each time BES Cyber System is used in the requirement parts. (This would be added to part 1.1, 1.2, and 1.2.5.) We also question why 1.2.1 and 1.2.2 is specific to "products or services provided to the Responsible Entity," but 1.2.4 is not. We recommend adding this phrase to 1.2.4: "Disclosure by vendors of known vulnerabilities related to products or services provided to the Responsible Entity." Further, we recommend further clarification to the term "vendor." We recommend explaining this term in the Guidelines and Technical Basis (GTB) section rather than the Rationale. The intent of the term "vendor" is not a Rationale for the standard. Additionally, there are a number of potential vendor scenarios which should be clarified in the GTB. The vendor explanation excludes other NERC Registered Entities, but it is not clear whether this exclusion also applies to other utilities not registered with NERC. It is also not clear whether the term vendor is intended to apply to contract employees, particularly those who may be using company issued computer equipment and receiving company developed security training. It would seem that the Transient Cyber Asset requirements already sufficiently mitigate this risk and additional requirements are not necessary. We also find that the term "system integrators" is not well understood and request further clarification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The main body text in Requirement R1 establishes applicability to high and medium impact BES Cyber Systems; the SDT believes repeating this applicability in the requirement parts is redundant. The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.	

Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	No
Document Name	
Comment	

Requirements 1.2 through 1.2.4. are extremely difficult to negotiate and implement with vendors, especially across such a diverse industry and diverse set of vendors. As written, the requirements make the vendor responsible for providing notifications to the Responsibility Entity. This puts the burden on the Responsible Entity to enforce these requirements through contractual obligations. The rationale states that "such contract enforcement is not subject to this Reliability Standard;" however, the performance of these requirements belongs solely to entities that are outside the jurisdiction of NERC and the Commission and can be held accountable only through contraction enforcement. As written, these specific reliability requirements put the Responsible Entities in a precarious position of acting as a surrogate regulator on a secondary industry.

If the intent is not to make the Responsible Entity accountable from a compliance stand point for the actions of vendors or other parties, the language should be written into the requirement wording. The clause in R2.2 states this exception, but does not then clarify what the Responsible Entity is obligated to do. The Responsible Entity is supposed to negotiate those terms, try to obtain that information, but if they can't then is it still not a violation? Will the auditors also look at it from this perspective?

Furthermore, the language of the R1.2 to R1.2.4 should be changed to meet the SDT's objectives while relying solely on the actions of the Responsible Entity and not those of any other party. However, if the intent is to include the items in R1.2 in the process for consideration of risk when selecting a vendor or product during the procurement process as the draft guidance seems to indicate, then those intentions should be explicit in the requirement language.

There is no issue with Requirement 3 requiring a periodic assessment of the supply chain cyber security risk management controls in order to update plans, etc. However, a recurring review by business unit stakeholders should be sufficient. The requirement to have the CIP Senior Manager or delegate approve the plan is simply a formality and is administrative in nature and provides no further security value.

Likes 0	

Dislikes 0	

Response. Thank you for your comments.

The SDT's approach in CIP-013-1 is in line with FERC Order No. 829, which stipulates that the standards should not impose obligations directly on vendors (P 36). The requirements provide responsible entities with flexibility to use tailored planning and procurement processes and do not obligate or hold the responsible entity accountable for vendor cooperation. The SDT believes the note in Requirement R2 establishes that terms and conditions, and vendor performance with contract provisions, are not in scope.
The SDT developed Implementation Guidance, which has been endorsed by the ERO Enterprise, to provide examples of compliant approaches to meet the requirements. As stated in NERC's approved Compliance Guidance Policy, "Registered entities can rely upon [the examples] and be reasonably assured that compliance requirements will be met."

The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of elements contained in the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. Examples are provided in the Implementation Guidance.

Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46).

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	

Comment

- Please provide clarification on what a "contract" is. For instance, is an annual software license a contract?
- Please provide feedback as to what Registered Entities should do if vendors refuse to the specifications within the CIP-013 requirements.

• Please provide further clarifications and expectations within Measure 2 to ensure entities are prepared for compliance oversight expectations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The objective of Part 1.2 is for entities to include the listed topics in their supply chain cyber security risk management plans so that procurement and contract negotiation processes address the applicable risks. Contracts a a type of procurement vehicle used to obtain products and services. An annual software license can be a type of contract. The requirements provide responsible entities with flexibility to use tailored planning and procurement processes and do not obligate or hold the responsible entity accountable for vendor cooperation. Responsible entities have flexibility to address vendor responsiveness. The SDT believes the evidence listed in Measure M2 covers the various types of evidence that an entity would use in implementing its supply chain cyber security risk management plan to plan and procure BES Cyber Systems. Correspondence, policy documents, or working documents that can show how the entity implemented processes such as those listed in the Implementation Guidance to plan and procure applicable BES Cyber Systems could be used as evidence.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
SPP offers comments on the subrequirements of R1, as follows:	

R1.1 – SPP recommends that subpart (i) be modified to accommodate the procurement "and/or" installation of vendor equipment "and/or" software and, further, requests clarification as to the intended meaning of the "transitions from one vendor(s) to another vendor(s)" concept within the context of subpart (ii).

1.2.1 – SPP recommends that "products or services" be modified to reference "products and/or services."

1.2.2 – SPP requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with any coordination component removed.

1.2.4 – SPP recommends that the 1.2.4 be modified to appropriately limit vendor disclosure of known vulnerabilities to the products and/or services provided to the Responsible Entity, consistent with 1.2.1. In addition, SPP notes that there is a lack of consistency between 1.2.1 and 1.2.4 with the use of the terms "vendor equipment" and "software" in 1.2.1, but uses the term "products" in subrequirement 1.2.4. SPP seeks clarification on whether the SDT intends "products" to be broader than equipment and software. SPP recommends that the SDT be consistent and use "vendor equipment" and "software" throughout, or provide additional clarification about the scope of the term "products."

1.2.6- SPP requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. SPP believes the "coordination of controls" may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, SPP is concerned that it is unclear what is required for "coordination," as well as how such coordination would be evidenced at audit.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT does not believe the suggested changes to Part 1.1 or 1.2.1 provide additional clarity.

The SDT has revised Part 1.2.4 for clarity. The SDT does not believe use of 'and/or' provides additional clarity.

The ERO Enterprise-endorsed Implementation Guidance lists examples of compliant approaches to Requirement R1 Parts 1.2, including 1.2.2 and 1.2.6. The SDT believes the standard and the examples in the Implementation Guidance provide the necessary clarity. Responsible Entities can provide additional detail in their Supply Chain Cyber Security Risk Management Plan.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

NRG offers comments on the sub requirements of R1, as follows:

R1.1 – NRG recommends that subpart (i) be modified to accommodate the procurement "and/or" installation of vendor equipment "and/or" software and, further, requests clarification as to the intended meaning of the "transitions from one vendor(s) to another vendor(s)" concept within the context of subpart (ii).

1.2.1 – NRG recommends that "products or services" be modified to reference "products and/or services."

1.2.2 – NRG requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with any coordination component removed.

1.2.4 – NRG recommends that the 1.2.4 be modified to appropriately limit vendor disclosure of known vulnerabilities to the products and/or services provided to the Responsible Entity, consistent with 1.2.1. In addition, NRG notes that there is a lack of consistency between 1.2.1 and 1.2.4 with the use of the terms "vendor equipment" and "software" in 1.2.1, but uses the term "products" in sub requirement 1.2.4. NRG seeks clarification on whether the SDT intends "products" to be broader than equipment and software. NRG recommends that the SDT be consistent and use "vendor equipment" and "software" throughout, or provide additional clarification about the scope of the term "products."

1.2.6- NRG requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. NRG believes the "coordination of controls" may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, NRG is concerned that it is unclear what is required for "coordination," as well as how such coordination would be evidenced at audit.

Additionally: NRG is concerned that the R1 guidance provides details which are beyond the scope of R1.

NRG requests that the NERC SDT consider re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. The Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing "identified to "acknowledged" or "confirmed."

Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.

Request more guidance for the term "vendor" and use cases. Guidance should prompt Entities to include their definition of "vendor" in their plan(s).

NRG recommends removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) that are covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear that there is a remaining need for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

NRG requests SDT consideration that: The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, NRG requests NERC SDT consideration of the assertion that Registered Entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

CIP-013-1 R1.2 – "One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable: " The term "as applicable" implies it is optional. Who determines whether something is applicable or not? NRG suggests that NERC SDT remove it or provide additional clarity.

CIP-013-1 R1.2.3, NRG has concerns that it is not clear when vendors have to notify if remote or onsite access should no longer be granted to vendor representatives. 2 hrs, 24 hrs, or 3 months?

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

1.1 – Delete "planning for". Or if the use of "planning for" in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting?

-

- R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. NRG requests SDT consideration of suggestion to delete.

Furthermore, NRG requests NERC SDT consideration of the following comments:

· On page 6 of CIP-013 draft:

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

NRG requests that industry have the ability to accept a level of risk through internal risk assessment processes if a supplier is unwilling to negotiate and accept the cyber security terms into negotiated contracts.

· On page 6 of CIP-013 draft:

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

NRG requests that the term vendor be further clarified to specify if meaning developers, product resellers or system integrators of "third-party" software, system components, or information system services, etc (versus internal company developers).

· On page 8 of CIP-013 draft (under R2):

NRG requests that the NERC standard drafting team consider providing additional clarification to the following paragraph:

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.

NRG requests further understanding of what, if any expectations are to be included in T&Cs and what are the expectations of how the vendor will be expected to perform as the term "expectations" is listed on page 6 of the standard?

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT does not believe the suggested changes to Part 1.1 or 1.2.1 provide additional clarity.

The SDT has revised Part 1.2.4 for clarity. The SDT does not believe use of 'and/or' provides additional clarity.

The ERO Enterprise-endorsed Implementation Guidance lists examples of compliant approaches to Requirement R1 Parts 1.2, including 1.2.2 and 1.2.6, that clarify the SDT's intent. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan. The ERO Enterprise endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. As previously stated, the ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. Accordingly, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." (See Compliance Guidance Policy on NERC's compliance page)

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance.

Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.

The SDT believes the cited paragraph "For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs) and in negotiations with vendors…", along with the note in Requirement R2, addresses the commenter's concerns regarding the responsible entity's obligation when vendors may be unable or unwilling to negotiate. Implementation Guidance provides additional examples of compliant approaches that are not dependent on vendor cooperation. The SDT believes the vendor description provided in the rationale addresses the commenter concerns about internal company developers. The rationale section states, in part: *The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services.* A responsible entity can provide further clarification in its supply chain cyber security risk management plan if the responsible entity deems it necessary. As indicated in the note for Requirement R2, the following are not in scope for CIP-013: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	No
Document Name	
Comment	
CIP-005 has had R2.4 and R2.5 added as they pertain to interactive user access and remote system to system access tracking. These were previously in the CIP-013 standard as part of the Supply Chain requirement. Due to CIP-005 R2 already dealing with an Intermediate system for Interactive Remote access, it seems logical that this requirement be expanded to include these. The clarification that we don't have and would like from NERC/WECC is the intent of the following statement in CIP-013 R1.2.5 ***"Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System".*** There is no Guidelines and technical basis at the end of the standard for this	

This has a very large implication as this says all software provided by a vendor has to perform an integrity and authenticity verification. This could implicate a dedicated channel from the vendor validating through software certificates which would imply entities forcing software vendors to provide this mechanism, which the likelihood of meeting this for MS, Symantec, (non-control system software) is slim. MD5 checksums can not validate the integrity of the software as this hashing mechanism was broken in 2005 (although a lot of software vendors still use it). So we need clarification on this before a vote recommendation can be established for CIP-013 R1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its procurement processes (such as in Requests for Proposal, contract negotiations, or other procurement processes). Part 1.2.5 does not obligate the responsible entity to obtain, or the vendor to provide, the means for performing software verification. 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 terms and conditions ultimately negotiated by the parties and included in a contract. As a result, actual contract terms are not in scope for CIP-013.	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
PJM agrees, with the following suggested edits:	

Within 1.2.1 and 1.2.2, PJM feels that "incident" need further clarification as it is a bit broad (i.e. could be interpreted as anything from a phishing attempt to an actual breach). PJM suggests it be narrowed down to actual breaches. Additionally, "security risk to the Responsible Entity" should be "security risk to the BES." Lastly, we like how the notification and coordination pieces are split out. *Within 1.2.3, PJM suggests changing "no longer be granted" to "should be revoked" to strengthen the language.* *Within 1.2.5, PJM suggests adding in "firmware" and "where the method to do so is available" as to match the CIP-010 language.*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested changes to Part 1.2.1 – 1.2.3 provide additional clarity. The SDT understands *firmware* to be a type of software. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
The understanding of the intent and purpose of CIP-013 is very dependent on the Implementation Guidance document. There is no guarantee that this document will be approved by NERC even if CIP-013 is approved. Request clarification on whether the SDT intends "products" to be broader than equipment and software. Recommend that the SDT be consistent and use "vendor equipment" and "software" throughout, or provide additional clarification about the scope of the term "products."	

There are concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, we recommend that all references to "contracts" and most references to "procurement" be struck from CIP-013, except the note in R2 that states:

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.

Our reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and achieve the protections required by R1.2. It is immaterial how these protections are achieved. Focusing thinking and audit approach on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such we ask that R1.2 be revised as follows:

1.2. *One or more process(es) used in procuring for its newly procured BES Cyber Systems that address the following elements, as applicable:*

("new" meaning obtained after the implementation of CIP-013).

Request that the term "elements" be included in R1.2, as shown above, to clearly align with the VSLs for this requirement.

Associated guidance in the "Rationale for R1" and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits or subtext in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately, there should be no expectation that such protections be achieved solely through the procurement process. The objective is achieving each protection, not in how it is achieved.

In the absence of such a change, we requests substantial additional clarification about how, without contract terms and contract negotiations being auditable, performance of R2 implementation will be audited and assessed.

Likes 0	
Dislikes 0	

Response Thank you for your comment.

The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities.

Vendor equipment and software are types of products. The SDT does not believe alternate wording for Requirement R1 provides additional clarity. A responsible entity may provide additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.

The SDT believes the requirements for procurement processes are necessary to address the Order No. 829 directives (P. 59). The proposed requirements provide flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

The SDT has revised the VSL for Requirement R2 to remove the word *element*.

The SDT believes the evidence listed in Measure M2 covers the various types of evidence that an entity would use in implementing its supply chain cyber security risk management plan to plan and procure BES Cyber Systems. Correspondence, policy documents, or working documents that can show how the entity implemented processes such as those listed in the Implementation Guidance to plan and procure applicable BES Cyber Systems could be used as evidence.

Implementation Guidance provides examples of processes to address Parts 1.2.1 and 1.2.2 that provide additional clarity. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.

Quintin Lee - Eversource Energy - 1

Answer	Yes
Document Name	
Comment	

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.

Recommend removing CIP-013 R1 subparts 1.2.5 and 1.2.6 from CIP-013 since these are covered in CIP-005 and CIP-010. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance “double jeopardy.”

The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed?

{C}1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it?

- What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting? - R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided examples of processes related to Part 1.2.1 through 1.2.6 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance. Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the proposed requirements in CIP-013-1 subject to the below requests for clarification and recommended revisions/additions. · AZPS requests that the SDT consider and provide guidance regarding the applicability of the requirements of CIP-013-1 where the traditional procurement process is not applicable to a particular purchase. For example, software that is purchased from a retail source rather than a vendor is often purchased subject to existing retail terms and conditions and without the opportunity to negotiate additional terms and conditions around the procurement. · AZPS further recommends the following changes/additions: · Requirement 1.2.4 - "Disclosure by vendors of known vulnerabilities ***when they become known to the vendor.***" · Requirement 1.2.5 as written is duplicative with CIP-010; hence, AZPS recommends this Requirement be deleted or revised to address the process for software integrity and authenticity, rather than actual verification of those.	

· Requirement 1.2.6 – AZPS recommends removal of the word “coordination” and on the insertion of the term “identification” to address a process for identifying how a vendor handles controls. · Requirement R2 – evidence may not be available for items that are purchased form a retail source, as noted above. AZPS recommends an exception be identified for this purpose.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Proposed CIP-013-1 requires responsible entities to develop and implement a supply chain cyber security risk management plan for BES Cyber Systems that addresses the specified planning and procurement processes. The proposed requirements provide flexibility for entities to develop a plan that includes various types of processes used for procurement by the responsible entity, and to address the applicable topics listed in Parts 1.2.1 through 1.2.6. The SDT does not believe the proposed revision to Part 1.2.4 is needed to meet the objective. A responsible entity can include the clarification in its supply chain cyber security risk management plan. The proposed requirement in CIP-010-3 is operational in nature and not related to procurement. Therefore the CIP-013 requirement is not duplicative of the CIP-010-3. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT does not believe the propose wording for Part 1.2.6 provides additional clarity. A responsible entity can include the clarification in its supply chain cyber security risk management plan. The SDT believes a responsible entity should use its supply chain cyber security risk management plan for all procurements of high and medium impact BES Cyber Systems, and be able to provide evidence for assurance purposes.	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	

Answer	Yes
Document Name	
Comment	
Modify R1.2.5 as follows: "Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System when technically feasible; and". This will help address concerns with vendors such as Microsoft that pushes patches when they identify a need. Add language to address allowable exception in the event of CIP Exceptional Circumstances for R2 (e.g. patches issued with ransomware attack in-progress needed immediate action to be taken). Luminant would prefer that the CIP-013 standard be formatted similar to other CIP standards with the use of tables (e.g.CIP-004-6 Table R1).	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R1 Part 1.2.5 does not require entities to perform software verification, so the SDT does not believe it is necessary to include *when technically feasible*. In implementing its processes in Part 1.2, the responsible entity is not required to include topics in 1.2.1 – 1.2.6 that are not applicable to the item being procured. This would include applications that are not technically feasible. Likewise, the SDT does not believe CIP Exceptional Circumstances apply to implementation of an entity's supply chain cyber security risk management plan. Implementation of elements contained in the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and negotiation processes. Performance of patch management is addressed in other reliability standards and not in scope of CIP-013. The SDT does not believe a table format would provide additional clarity.	

Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG request clarification, regarding R1.2.4, of whom the vulnerability must be known by to require disclosure and that it only be for the vendor's own products and only those supplied to the Responsible Entity. As stands, it might be interpreted that vulnerabilities might not need to be disclosed until publicly known, for products the Responsible Entity doesn't have, or for vulnerabilities the vendor might know in products other than its own. Suggest changing to "Disclosure by the vendor of vulnerabilities known to the vendor concerning products and services supplied by the vendor to the Responsible entity. Requirement R1 Part 1.2.4 requires additional clarification for the type of "known vulnerabilities" Vendor definition is required to avoid ambiguity; does the term vendor apply for contract employees/augmented staff/outsourcers?	

Are the requirements R1-R3 enforceable in exceptional circumstances?	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT agrees that Part 1.2.4 should be clarified to apply to 'products or services provided to the Responsible Entity' and has added this clarification Part 1.2.4 in Draft 3 of proposed CIP-013-1. A responsible entity can provide additional clarity if the responsible entity believes it is necessary in its cyber security supply chain risk management plan.

The rationale section, including vendor description, becomes part of the guidelines section of the standard following board adoption. An entity can provide additional clarification of vendor relationships in its plan. Requirement R1 Part 1.2 pertains to procuring BES Cyber Systems, which the SDT does not believe would entail staff augmentation contractors. Responsible entities should consider entity-specific circumstances related to staff augmentation contractors or procurement of products or services from non-NERC utility in developing their plan.

The SDT considered whether to include provisions for CIP Exceptional Circumstances in Proposed CIP-013-1, but determined that the exceptions were not appropriate because CIP-013-1 addresses planning and procurement processes.

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
ACES supports the requirements to reduce the risk of remote access management. Using the CIP Applicability Section reduces the previous confusion of what BES Cyber Assets are in scope.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	

Concerned that the R1 guidance provides details which are beyond the scope of R1

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?

In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. Suggest changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Recommend removing those items (CIP-013 R1 subparts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013. There are substantive requirements being incorporated into CIP standards to perform functions for all BES Cyber Systems (to the extent possible), it is not clear there is a remaining need to for a separate standard requiring that those items be addressed during the procurement process. This appears to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having a standard that requires you to perform

the underlying function and also to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy." The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy. Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed? 1.1 – Delete "planning for". Or if the use of "planning for" in R1 creates a necessary distinction between 1.1 and 1.2, what is it? - What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn't a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting? - R1.2.2: "Coordination of responses to vendor-identified incidents….", it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comments. The examples provided in the Implementation Guidance demonstrate a way, but not the only way, of being compliant with CIP-013-1. The SDT believes the examples are in scope. Responsible entities are not obligated to use approaches in the Implementation Guidance. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore	

the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
See below comments.	
Likes 0	
Dislikes 0	
Response	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. These Parts appear to be duplicative. Guidance does not adequately distinguish between the Parts. One interpretation is that Part 1.2.1 is for products/services and that Part 1.2.4 is for vulnerabilities in the product. It is not clear if these Parts expect information sharing at the time of procurement or on-going?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has provided examples of processes related to Part 1.2.1 through 1.2.6 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
The Registered Entity suggests consider revising Section 1.2.3 to clarify under what circumstances vendors would be expected to notify the Registered Entity that vendor remotes access should be revoked. Regarding Section 1.2.4, suggest revising to clarify what type of vulnerabilities would be included in this disclosure.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT clarified Part 1.2.4 to apply to 'products or services provided to the Responsible Entity'. The SDT has provided examples of processes related to Part 1.2.3 in the Implementation Guidance. A responsible entity may provide any additional clarity that the responsible entity believes is needed in its supply chain cyber security risk management plan.	

Bob Thomas - Illinois Municipal Electric Agency – 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
R1-R2 are clearly stated and provide for the development and implementation of the required CIP-013-1 cyber security plans. R3 sets a clear expectation for periodic reviews and approvals. From an auditor's perspective, requiring the first review and approval of the R1 plan on or before the effective date of CIP-013-1 (Implementation Plan, Initial Performance of Periodic Requirements section, p. 3) provides clear guidance to industry on implementation expectations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	

Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Regarding the use of the term “vendor,” as described in the “Rationale for Requirement R1” section of CIP-013-1: the SDT may want to clarify that staff augmentation contractors are not considered to be “vendors” in the context of the standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	

Comment
What is the difference between 1.2.1 and 1.2.4? Why is the scope of 1.2.2 limited to vendor-identified incidents? What if a third party identifies an incident? Is there an expectation of the vendor to disclose non-public information in 1.2.4? Is this only during contracting or is there an expectation of new vulnerabilities to be disclosed? 1.1 – Delete “planning for”. Or if the use of “planning for” in R1 creates a necessary distinction between 1.1 and 1.2, what is it? - What is implied by *(ii) transitions from one vendor(s) to another vendor(s)*? Why is this distinction necessary? Wouldn’t a vendor transition require a new contract? Does this refer to the act of severing existing remote access permissions? Subcontracting? - R1.2.2: “Coordination of responses to vendor-identified incidents….”, it is not clear who should be doing the coordinating and why this is necessary. Suggest deleting.
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Examples for all of the parts in Part 1.2 are included in the Implementation Guidance. *Incidents* (Part 1.2.1) could be a security breach at a vendor; *vulnerabilities* (1.2.4) could be a product security flaw. Responsible entities can provide additional clarifications in their Supply Chain Cyber Security Risk Management Plans. Part 1.2.2 specifies that the responsible entity must have process used in procurement to address coordination of responses to vendor-identified incidents. The term *vendor-identified* is used because to indicate that the objective is to address those incidents that arise with the vendor from which the product or service is being procured. A responsible entity could choose to use alternate terms, such as third-party, or expand the scope in its Supply Chain Cyber Security Risk Management Plan.	

Part 1.1 and Part 1.2 address distinct directives from Order No. 829 pertaining to planning and procurement, respectively. (see Rationale and Order No. 829 P. 56 and P.59). Examples of processes or activities that could address the objectives for both are contained in the Implementation Guidance. Per Part 1.1, responsible entities must have process(es) that they use when planning for procurement of BES Cyber Systems to consider cyber security risks to the BES that could arise from transitions from one vendor to another vendor. The intent is for the responsible entity to consider cyber security risks that may result from the change in vendor, which may inform the entity's procurement process.

Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
With respect to the proposed Requirement 1 Part 1.2.1, compliance requires the vendor to be responsive to vendor-identified incidents. We can only be compliant if the vendor releases such information. We can't be held responsible for a vendor that does not provide incident related information. This verbiage has to be deemed acceptable when developing the plan(s). With respect to the proposed Requirement 1 Part 1.2.4, compliance requires the vendor to be responsive to disclosing vulnerabilities. We can only be compliant if the vendor releases such information. We can't be held responsible for a vendor that does not disclose vulnerabilities. This verbiage has to be deemed acceptable when developing the plan(s). With respect to the proposed Requirement 1 Part 1.2.5, compliance requires cooperation by the vendor to participate in such a program. We will give procurement preference to vendors willing to participate however we are still at relying on vendor cooperation. We can't be held responsible for a vendor that does not provide accurate verification of software integrity and authenticity. This verbiage has to be deemed acceptable when developing the plan(s).	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. Vendor performance or response does not determine responsible entity compliance with any parts in Part 1.2. Examples of compliant approaches are included in the Implementation Guidance.	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
We support the comments submitted by APPA, including the following recommendations: Re-word R1, Parts 1.2.1 and 1.2.4 to better describe what is expected. The endorsed Guidance does not adequately distinguish between the two parts. "Vendor" is not a NERC-defined term and contributes ambiguity. Those items (CIP-013 R1, Parts 1.2.5 and 1.2.6) covered in CIP-005 adn CIP-010 should be removed from CIP-013 to avoid duplication. The Compliance and/or Implementation Guidance should make clear that, when evidence demonstrates that all items expressly identified in CIP-013 R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. There is concern about language related to procurement contracts, specifically the use of master agreements, piggyback agreements, and evergreen agreements. All references to "contracts" and most references to 'procurement" should be struck from CIP-013, except the note in R2.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

The SDT revised Part 1.2.4 for consistency with other parts in Part 1.2. The SDT believes Part 1.2.1 and 1.2.4 meets the reliability objective of Order No. 829 and that the endorsed Implementation Guidance provides additional clarity by describing examples of compliant approaches to meet these parts. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
: Platte River Power Authority (PRPA) continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013. PRPA agrees with limiting the requirement to high and medium assets only.	

R1: PRPA generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

PRPA recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: PRPA agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

R3: PRPA agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, PRPA proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore

the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." The SDT agrees that the ERO roll-out strategy for CIP-013 following regulatory approval should include activities to help responsible entities develop and assess their plans and promote consistency in audit approaches.	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
For Requirement R 1, Part 1.2.4, CenterPoint Energy Houston Electric, LLC ("CenterPoint Energy") recommends the following modification to help clarify the type of disclosed vulnerabilities: "Disclosure by vendors of known security vulnerabilities involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System."	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

The SDT revised Part 1.2.4 for consistency with other parts in Part 1.2. The SDT does not believe it is necessary to include 'or its supply chain' in the requirement since this could be covered by the requirement as written. A responsible entity could include such a clarification in its plan if the responsible entity so desires.	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Even though the second proposed version of this standard has been simplified, SDG&E believes compliance with CIP-013-1 is potentially difficult and costly to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

SMUD continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

SMUD agrees with limiting the requirement to high and medium assets only.

R1: SMUD generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a Technical Feasibility Exception (TFE) or Asset Capability Exception, should be included in the standard for these kinds of procurement activities. An additional consideration is to allow agreements between the vendor and entity that will not cause a financial impact, such as a letter of understanding, commitment to a plan of action or other agreement.

SMUD recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	

Austin Energy (AE) supports efforts to ensure the security of the Bulk Electric System and appreciates the time and effort the SDT put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

AE agrees with limiting the requirement to high and medium assets.

R1: AE generally agrees with the proposed R1 but has concerns about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and "piggyback" agreements. NERC should include an exception, comparable to a CIP Exceptional Circumstance, for such procurement activities.

AE recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required “when the method to do so is available” by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts which require entities to perform the underlying function and take those functions into account during the procurement process is needless duplication which does not increase security or reliability and could result in compliance “double jeopardy.”

R2: AE agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in R1.

R3: AE agrees a 15-month review period is appropriate to review the supply chain cyber security risk management plan in R1.

Additionally, AE proposes the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date, similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response Thank you for your comments. Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." The SDT agrees that the ERO roll-out strategy for CIP-013 following regulatory approval should include activities to help responsible entities develop and assess their plans and promote consistency in audit approaches.
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments	

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The proposed requirements provide flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples. Some situations, such as when contracts are negotiated on behalf of the responsible entity, could be met by providing input to parties negotiating on behalf of the responsible entity. Proposed CIP-013 does not preclude responsible entities from taking other actions suggested by the commenter to pursue cyber security protections.

The SDT does not believe removing the procurement and contracting process from the scope of the proposed standard would meet the project SAR and directives in Order No. 829, which direct NERC to develop standards to "require entities to develop and implement a plan that includes security controls for supply chain management" (P. 43) and to include certain procurement controls (P. 45). The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP, vendor negotiations, or input into cooperative agreements. Evidence could include RFPs or other procurement correspondence that demonstrate the responsible entity's cyber security risk management concepts and controls. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21).

The SDT developed Implementation Guidance, which has been endorsed by the ERO Enterprise, to provide examples of compliant approaches to meet the requirements. As stated in NERC's approved Compliance Guidance Policy, "Registered entities can rely upon [the examples] and be reasonably assured that compliance requirements will be met."

The SDT clarified Part 1.2.4 to apply to 'products or services provided to the Responsible Entity' for consistency with other parts in Part 1.2. Examples of approaches for Part 1.2.1 through 1.2.6 are provided in Implementation Guidance. Responsible entities can provide additional clarification in their supply chain cyber security risk management plans.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans. Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Concerned that the R1 guidance provides details which are beyond the scope of R1 Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.	

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s). Request re-wording of R1 Part 1.2.1 and 1.2.4 to easily understand what is expected. In R1 Parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. Request to merge R1 Part 1.2.1 and 1.2.2 for the notification and the coordination related to vendor-identified incidents. Request to merge R1 Part 1.2.3 and Part 1.2.6 for the notification and the coordination of controls when remote or on site access are required and granted for (i) vendor-initiated interactive remote access, and (ii) system-to-system remote access with a vendor(s). The Compliance and/or Implementation Guidance should make clear that, as long as evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity’s procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs. The SDT agrees that some responsible entities may need to provide additional entity-specific clarifications in their cyber security risk management plans.

The SDT clarified Part 1.2.4 to apply to ‘products or services provided to the Responsible Entity’ for consistency with other parts in Part 1.2.

The SDT does not believe merging certain parts in Part 1.2 provides additional clarity.

The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations."	
Theresa Allard - Minnkota Power Cooperative Inc. - 1	
Answer	Yes
Document Name	
Comment	
See MRO NSRF comments.	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.	

SRP agrees with limiting the requirement to high and medium assets only.

R1: SRP generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, should be included in the standard for these kinds of procurement activities.

SRP recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: SRP agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

R3: SRP agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, SRP proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Proposed Requirement R1 provides flexibility for entities to develop a plan that includes procurement processes for various types of procurement activities including multi-party wide-area contracts, master agreements and piggyback agreements. The SDT believes that an exception is not needed because of the flexibility provided in the requirements. The SDT has revised the rationale to include types of procurement activities listed by the commenter among the other examples.

Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. The ERO Enterprise's endorsement of the Implementation Guidance examples means the ERO Enterprise CMEP staff will give these examples deference when conducting compliance monitoring activities. As stated in the compliance guidance policy, "Registered entities can rely upon the example and be reasonably assured that compliance requirements will be met with the understanding that compliance determinations depend on facts, circumstances, and system configurations." The SDT agrees that the ERO roll-out strategy for CIP-013 following regulatory approval should include activities to help responsible entities develop and assess their plans and promote consistency in audit approaches.	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Even though the second proposed version of this standard has been simplified, SDG&E believes compliance with CIP-013-1 is potentially difficult and costly to demonstrate compliance.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While in overall agreement with Requirements 1 through 3, ACEC does have the following concern: The R1 and R2 requirements in the draft split the development of one or more documented supply chain cyber security risk management plan(s) (R1) and the implementation of those supply chain cyber security risk management plan(s) specified in Requirement R1 (R2). By splitting these the potential for violations have been increased from one (1) to two (2) – one for each requirement. It is recommended that R1 and R2 be combined to reduce the potential of multiple violations for what should be a single Requirement. To illustrate, a majority of the Standards have their development of plans, processes, or procedures and implementation of those plans, processes, or procedures in the same requirement: CIP-002-5.1 R1; CIP-003-6 R2, R4; CIP-004-6 R1, R2, R3, R4, R5; CIP-005-5 R1, R2; CIP-006-6 R1, R2, R3; CIP-007-6 R1, R2, R3, R4, R5; CIP-010-2 R1, R2, R3, R4; CIP-011-2 R1, R2	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. In developing the 2nd draft of proposed CIP-013-1, the SDT separated requirements for responsible entities to develop and implement their Supply Chain Cyber Security Risk Management Plans. The SDT believes this approach to CIP-013-1 clarifies the obligations and more straightforward for responsible entities.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	

Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
During the CIP-013-1 webinar on Feb 2, the SDT indicated several times that it is not the intention of R1 to force vendors to perform actions so that entities can comply with the standard. R1.2.1, R1.2.2, R1.2.3, R1.2.4 would force vendors to develop internal processes to notify entities of any changes relating to the requirements which would force vendors to take independent action to notify entities of any changes. Also, during the procurement phase, why would vendors reveal potential security flaws in their product above and beyond normal security patch notifications while they are competing against other vendors for the entities business? Also, entities have processes in place already for other CIP requirements to fully prepare an asset for deployment into the ESP. We don't grab equipment off of the back of the delivery truck and deploy it into the ESP immediately so what is the point of knowing about security flaws in their products during procurement? Any security flaws are probably already addressed with patches that will be downloaded and installed when preparing the asset for deployment. Also, a vulnerability assessment has to be performed against the asset and CIP-007/CIP-005 security controls have to be checked prior to deployment. 1.2.1, 1.2.2, 1.2.4, 1.2.5 appear to be redundant with CIP-007 R2 security patch management. Is the SDT expecting vendors to provide information about security/design flaws above and beyond the normal security patch notifications? If so, what kind of information would that be? 1.2.5 is troublesome as well (and it seems to be a duplicate of CIP-010-3 R1.6). Entities typically use update or proxy servers to discover and identify applicable security patches. For example, some use Windows Update Server Services to identify patches and roll them out	

once testing and approvals are complete. Do we need to check the check sums of the identified patches or can we trust that the update servers are authenticating the software?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirement as written accomplishes the reliability objectives contained in the project SAR and FERC Order No. 829. The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP or vendor negotiations. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21). The note in Requirement R2 excludes contracts because they may contain business-sensitive information, and because the responsible entity may not be able to obtain all security provisions in Parts 1.2.1 – 1.2.6 with all vendors since the requirements cannot 'directly impose obligations on suppliers, vendors, or other entities". Requirement R1 Parts 1.2.5 and 1.2.6 address procurement processes related to software verification and vendor remote access, respectively. The approved requirements for security patch management in CIP-007 and proposed requirements in CIP-010-3 and CIP-005-6 are operational in nature and not related to procurement. Therefore the CIP-013 requirements are not duplicative of the CIP-010-3 and CIP-005-6 requirements. The SDT believes both operational and procurement related controls provide reliability benefit and are needed to address the directives in Order No. 829.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

There is a lack of consistency between R1 parts 1.2.1 and 1.2.4 with respect to the use of the terms. While part 1.2.1 uses the “vendor equipment” and “software,” part 1.2.4 uses the term “products.” The SDT should clarify if it intends “products” to be broader in scope than equipment and software. USI recommends that the SDT be consistent and use “vendor equipment” and “software” throughout, or provide additional clarification about the scope of the term “products.”

In R1 parts 1.2.1 and 1.2.2, the term “vendor-identified incident” is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor. It could mean only incidents identified by the vendor. USI suggests changing “identified to “acknowledged” or “confirmed.”

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005.

USI believes the SDT should provide guidance regarding the use of the term “vendor.” If “Vendor” is not defined by NERC, the Guidance should recommend that Entities include their definition of “vendor” in their plan(s).

Associated guidance in the “Rationale for R1” and in the separate implementation guidance should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no function in auditing. Contract terms might be used by an entity as evidence of performance, but there should be no expectation by audits or subtext in the Standard or implementation guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately there should be no expectation that such protections be achieved solely through the procurement process. Consistent with performance-based standards the objective is achieving each protection, not in how it is achieved.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comment.

The SDT has addressed any inconsistent terms in parts 1.2.1 – 1.2.6 as appropriate.

The SDT does not believe changing 'identified' to 'confirmed' in part 1.2.1 provides additional clarity to the requirement. Responsible Entities have flexibility to tailor their supply chain cyber security risk management plans for clarity where deemed appropriate by the Responsible Entity. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. The SDT does not agree that the guidance should recommend entities develop their own definition of vendor because entities can use the description that is included in the rationale. However, if an entity determines additional clarity is needed, they may provide such clarity in their supply chain cyber security risk management plan. Proposed CIP-013-1 contains *risk-based* requirements to mitigate cyber security risks to the BES in the supply chain of BES Cyber Systems in accordance with the project SAR and Order No. 829. The commenter's approach suggests removing the procurement and contracting process from the scope of the proposed standard. Such an approach would not meet the directives in Order No. 829, which direct NERC to develop standards to "require entities to develop and implement a plan that includes security controls for supply chain management" (P. 43) and to include certain procurement controls (P. 45). The intent is for responsible entities to accomplish the objective by including the security topics contained in Requirement R1 Parts 1.2.1 – 1.2.6 in the entity's procurement processes, such as RFP or vendor negotiations. Evidence could include RFPs or other procurement correspondence that demonstrate the responsible entity's cyber security risk management concepts and controls. Consistent with the Order, the standard obligates responsible entities to address supply chain cyber security risk management without "directly impos[ing] obligations on suppliers, vendors or other entities that provide products or services to responsible entities" (P. 21). .

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	

Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
ITC Holdings agrees with the proposed requirements, however, we believe the wording of CIP-013 leaves a lot of room for interpretation. We recommend being more prescriptive in the wording of CIP-013 as well as providing detailed guidance in the Technical Guidance document. Additionally, ITC Holdings agrees with the below comment submitted by SPP regarding the use of "coordination": 1.2.6- SPP requests clarification as to the "coordination" intended to be imposed, suggesting that the requirement may stand alone with the coordination component removed. SPP believes the "coordination of controls" may be interpreted as requiring the Responsible Entity and vendor to jointly develop and/or coordinate controls, rather than simply requiring the Responsible Entity to address the requisite remote access controls in its supply chain cyber security risk management plan(s). As drafted, SPP is concerned that it is unclear what is required for "coordination," as well as how such coordination would be evidenced at audit.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT's intent with proposed CIP-013-1 is to address the reliability objectives in the project SAR and Order No. 829 in a non-prescriptive manner. To provide a clear example of compliance with the standard, the SDT developed Implementation Guidance what has been endorsed by the ERO Enterprise in accordance with NERC's Compliance Guidance policy.	

The ERO Enterprise-endorsed Implementation Guidance lists examples of compliant approaches to Requirement R1 Part 1.2, including 1.2.2 and 1.2.6. The SDT believes the standard and the examples in the Implementation Guidance provide the necessary clarity. Responsible Entities can provide additional detail in their Supply Chain Cyber Security Risk Management Plan.
Wesley Maurer - Lower Colorado River Authority - 5

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	

David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	

Requirement R1. The IRC has no issues with the concept. We offer a recommendation on the language, "(i) Responsible Entity procures and installs vendor equipment and software; and (ii) Responsible Entity transitions from one vendor(s) product or service to another vendor(s) product or service".

Note: **ERCOT does not support the above comment.**

Requirement 1.2.1. The current wording suggests that the vendor has sufficient knowledge of the Responsible Entities' environment to know that a particular vulnerability does in fact pose a security risk to the Responsible Entity. We offer a recommendation on the language, *"Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that could pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.2. The current phrase "coordination of response" is not clear as to what is intended by "coordination". We offer a recommendation on the language, *"Coordination of response activities by the vendor and the Responsible Entity to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;"*

Requirement 1.2.4. The current wording is not clear as to which vulnerabilities are applicable. We offer a recommendation on the language, *"Disclosure by vendors of known vulnerabilities in the procured product or service following a responsible disclosure process"."*

Requirement 1.2.6. The use of the phrase "Coordination of controls" is confusing. We offer a recommendation on the language, *"Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s)."*

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT believes Parts 1.2.1 – 1.2.6 describe the cyber security risk topics that must be included in each responsible entity's Supply Chain Cyber Security Risk Management Plan for use in procuring BES Cyber Systems. Responsible entities can tailor specific wording in their plan to meet their procurement needs or to conform to the responsible entity's cyber security policies, plans, and practices.	
IESO	
Answer	No
Document Name	
Comment	
The IESO agrees in principle with the proposed requirements and respectfully submit suggestions for purposes of clarity. Requirement 1.2.1 We suggest the following wording change as the current wording suggests that the vendor has sufficient knowledge of the Responsible Entities' environment to know that a particular vulnerability does in fact pose a security risk to the Responsible Entity. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that *could* pose cyber security risk to the Responsible Entity; Requirement 1.2.2 We suggest the following wording change as the current phrase "coordination of response" is not clear as to what is intended by "coordination". Coordination of response *activities by the vendor and the Responsible Entity* to address vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	

Requirement 1.2.3 We suggest the following wording change as the current wording suggests that the Vendor has sufficient knowledge of the Responsible Entity to determine whether or not an individual should no longer be granted access. The Responsible Entity is the only party to an agreement that has the ability to determine who should or should not have access. *Circumstances where vendors should notify the Responsible Entity that access requirements of the vendor or third party personnel has changed.* Requirement 1.2.4 We suggest the following wording change as the current wording is not clear as to which vulnerabilities are applicable. Disclosure by vendors of known vulnerabilities *in the procured product or service;* Requirement 1.2.6 We suggest the following wording change as the use of the phrase “Coordination of controls” is confusing. Controls for; (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes Parts 1.2.1 – 1.2.6 describe the cyber security risk topics that must be included in each responsible entity’s Supply Chain Cyber Security Risk Management Plan for use in procuring BES Cyber Systems. Responsible entities can tailor specific wording in their plan to meet their procurement needs or to conform to the responsible entity’s cyber security policies, plans, and practices.	
Richard Vine - California ISO - 2	
Answer	

Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank for your comment.	
W. Dwayne Preston - Austin Energy - 3	
Answer	
Document Name	
Comment	
I would support the comments of Andrew Gallo Austin Energy for all questions.	
Likes 0	
Dislikes 0	
Response. Thank for your comment.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	

MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank for your comment.	

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	

ERCOT joins the comments of the IRC and offers the following additional comments:

Regarding Part 2.4, ERCOT is concerned that the meaning of "determining" in the phrase "have one or more methods for determining active vendor remote access sessions" is unclear. If the SDT's intent is to require *identification* of instances of active vendor remote access, ERCOT suggests rewording to "have one or more methods of *identifying instances of* active vendor remote access (including Interactive Remote Access and system-to-system remote access)."

ERCOT also requests clarification on the meaning of "system-to-system remote access." Interpreted broadly, this requirement could mean all ingress/egress network connections to the security zone. Identifying each instance of connection could become extremely burdensome, without providing any meaningful reliability benefit.

ERCOT recommends that the meaning of system-to-system remote access be qualified as vendor remote access which can do harm to the BES Cyber System (BCS) and recommends the following language:

"Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access). This is limited to sessions which have the ability to harm the BCS."

If the SDT declines to adopt this language, the SDT should consider defining "system-to-system remote access" or further clarifying the meaning of this term in the "Guideline and Technical Basis" section or in the Implementation Guidance.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The SDT does not believe replacing *determining* with *identifying instances* provides additional clarity. Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor. The SDT does not support the suggested change to include the sentence *This is limited to sessions which have the ability to harm the BCS* because the sentence could be inconsistently interpreted. The SDT believes the measures provide a list of some methods that can achieve the reliability objective without excessive burden on the Responsible Entity. For example, methods for accessing logged or monitoring information to determine active vendor remote access sessions may leverage existing entity processes.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	

See comments in attached file (comment at end of document)	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	No
Document Name	
Comment	
It remains unclear to us as to what the phrase “system-to-system” is meant to include. Please define or provide examples of what would be considered vendor “system-to-system” remote access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to “user-initiated access by a person”, the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor	
Timothy Reyher - Eversource Energy – 5	

Answer	No
Document Name	
Comment	

Comments:

The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question.

Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-013.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard.

The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	

Duke Energy requests additional clarity pertaining to the use of the term “active” in Requirement 2 Parts 2.4 and 2.5. As written, it could be interpreted that an entity would be required to monitor the remote access sessions of a vendor in real-time. Was this the drafting team’s intent with this language? If the drafting team’s intent was that an entity only be able to identify which vendor’s have remote access, we suggest revising the standard to more closely reflect said intent. If it is the drafting team’s intent that an entity must monitor in real-time the remote access of a vendor, additional guidance as to acceptable methods to achieve compliance with this intent is necessary.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT’s intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include:

- *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;*
- *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or*
- *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*

Don Schmit - Nebraska Public Power District – 5	
Answer	No
Document Name	
Comment	
NPPD supports the comments for the MRO NSRF for this question.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Nicholas Lauriat - Network and Security Technologies – 1	
Answer	No
Document Name	
Comment	
Suggest rewording 2.4 to read, “Have one or more methods for determining when vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) are active.” Alternative wording would be, “Have one or more methods for identifying active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested changes provide additional clarity.	

Wendy Center - U.S. Bureau of Reclamation – 5	
Answer	No
Document Name	
Comment	
Reclamation recommends that CIP-005-6 Requirement R2 Part 2.4 Requirements be changed to state, “Have one or more methods for determining and logging active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).” Reclamation recommends that the first bullet in CIP-005-6 Requirement R2 Part 2.4 Measures be changed to state, “Methods for accessing logged and actively monitored information to determine active vendor remote access sessions;” Reclamation also recommends that CIP-005-6 R2.3 be changed to "Where technically feasible, require multi-factor authentication for all Interactive Remote Access sessions" to align with CIP-007 R5, dealing with authentication requirements to help with consistency within the standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed Part 2.4 and 2.5 address the objectives contained in the project SAR and Order No. 829. These objectives are aimed at establishing controls on vendor remote access to BES Cyber Systems, covering both user-initiated and machine-to-machine vendor remote access, to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES (P. 51). The SDT does not believe the requirement needs to include logging to meet the objective. The SDT also does not believe the suggested change in M2 to *actively* monitored information improves the clarity of the requirement or effectiveness in addressing the objective. Modifying Requirement R2 Part 2.3 to address technical feasibility is not in scope for Project 2016-03 per the project SAR.	

Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	No
Document Name	
Comment	

CIP-005-6 R2 Part 2.4 as drafted does not identify the "direction" of how system-to-system remote access is initiated. Interactive Remote Access specifies that it originates "from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeters". Without defining the system of origin or other defining controls, similar to the definition of Interactive Remote Access, any connection from a CIP Cyber Asset to a vendor system, even if one-way and simply for data acquisition/submission, could be interpreted as subject to this requirement. Additional clarification is requested.

Additionally, the Supplemental Material for the requirement points to a separate document without an official link. It appears this document has not been updated in six (6) years, and mostly targets securing Interactive Remote Access. It is requested that updated relevant material be placed in the Standard's Supplemental Material section, similar to other CIP standards, and that the Supplemental Material section also attempt to provide guidance on the securing of system-to-system remote access.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors, regardless of origin. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor

The SDT has provided relevant information in the rationale section, which will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT believes Requirements R2 Part 2.4 and 2.5 and the accompanying measures, along with the rationale, provide the information necessary for entities to meet the reliability objective.	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
I fully support the concept of monitoring and being able to terminate all remote acccess sessions, however as written the additional requirements have no timing aspects associated with them, have no component for notification or alerting on active sessions, are atrifically limited to vendor access only, (lower case vendor) so may not include contractors, service providers, etc. Cannot support the requirement as written.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes the proposed requirements as written provide reliability benefit and address the Order No. 829 directives. Furthermore, CIP-005-6 Requirement R1 Part 1.5 provides a mechanism for Responsible Entities to determine when a response to suspicious activity in a vendor remote access session may be warranted. Part 1.5 requires Responsible Entities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Detections associated with this requirement could provide the triggering mechanism for Part 2.4.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
With the deletion of the language in R2, it now appears that every Responsible Entity needs to have a documented process for Interactive Remote Access, even if the Responsible Entity does not allow it. Why did the team delete this exemption language from R2 as it seemed to lessen the burden for those entities that do not allow Interactive Remote Access?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT developed Proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address Order No. 829 directives for vendor remote access controls with input from the Project 2016-02 CIP Revisions SDT. The scope of the revised requirement R2 is expanded to address all remote access management, not just Interactive Remote Access. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the Rationale section.	
Thomas Foltz - AEP – 5	
Answer	No
Document Name	
Comment	
R2 part 2.4 should read: Have one or more methods for determining when vendor Interactive Remote Access and/or vendor system-to-system remote access sessions are active. Part 2.5 should read: Have one or more methods to disable active vendor Interactive Remote Access and/or vendor system-to-system remote access sessions).	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested change provides additional clarity.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

The inclusion of (including Interactive Remote Access and system-to-system remote access) is problematic as the NERC defined term of Interactive Remote Access (IRA) explicitly excludes system-to-system process communication. Additionally, IRA already includes the concept of vendors (see 3) below).

"User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications."

The SDT should consider removing this system-to-system exclusion from the IRA defined term and stating Part 2.4 as –

Have one or more methods for determining active vendor Interactive Remote Access sessions.

And Part 2.5 as –

Have one or more method(s) to disable active vendor Interactive Remote Access sessions.

(note: the addition of 'sessions' in this Part to be consistent with Part 2.4.)

Lastly, from an SCRM perspective, the SDT should consider at least including some indication of when vendor remote access could or should be disrupted, but that may be better addressed in the CIP-013-1 R1.2.2 and/or R1.2.6 processes of the SCRM plan(s).	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that revising the definition of IRA could have met the objective. However because the scope and application of the IRA term is beyond the scope of Project 2016-03, the SDT decided to address the vendor remote access objectives by using the approved defined term and adding system-to-system vendor remote access in the requirements. Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. The SDT believes CIP-005-6 Requirement R1 Part 1.5 provides a mechanism for Responsible Entities to determine when a response to suspicious activity in a vendor remote access session is warranted. Part 1.5 requires Responsible Entities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	
Richard Vine - California ISO – 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Franklin Lu - Snohomish County PUD No. 1 – 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Please clarify definition of system-system communications.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to "user-initiated access by a person", the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

There needs to be a clear explanation of “machine-to-machine” and “system-to-system” remote access in the Guidelines & Technical Basis to provide the necessary understanding and scoping of these concepts for industry.

For example – “Machine-to-machine” or “system-to-system” remote access would include a logical connection between a High or Medium Impact BES Cyber System or it’s associated PCAs into or out of the associated ESP with a vendor-maintained Cyber Asset, and that connection does not have an interactive user access capability.

Additionally, under the Measures of R2.4, the statement of examples needs to have “such as” following “(including Interactive Remote Access and system-to-system remote access), such as:” to make it clearer that the below bulleted items are options an entity may choose from, and to be consistent with the formatting of R2.5.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT is including the following clarification of vendor remote access in the rationale section to support Requirement R2 Parts 2.4 and 2.5: *Active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i)is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.* The rationale section remains with the approved standard.

The SDT has made the suggested change to the Measure for Part 2.4.

David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The IRC agree with the new CIP-005-6 Requirement R2 Parts 2.4 and 2.5 however we note there is no corresponding "Guidance and Technical Basis" or "Rationale". We also suggest that guidance be drafted to help entities understand what is intended by the term "Vendor" in relation to parts 2.4 and 2.5. Regarding Part 2.4, the IRC is concerned that the meaning of "determining" in the phrase "have one or more methods for determining active vendor remote access sessions" is unclear. If the SDT's intent is to require *identification* of instances of active vendor remote access, the IRC suggests rewording to "have one or more methods of *identifying instances of* active vendor remote access (including Interactive Remote Access and system-to-system remote access)."	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has provided relevant information in the rationale section, which will become part of the supplemental material following NERC Board adoption of the proposed standard. Rationale includes a description of vendor. Upon adoption of the standard by the NERC Board of Trustees, this information will be transferred to the guidelines section of the standard. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The SDT does not believe replacing *determining* with *identifying instances* provides additional clarity.	
IESO	
Answer	Yes

Document Name	
Comment	
The IESO agree with the new CIP-005-6 Requirement R2 Parts 2.4 and 2.5 however we note there is no corresponding “Guidance and Technical Basis” or “Rationale”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has provided relevant information in the rationale section, which will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT believes Requirements R2 Part 2.4 and 2.5 and the accompanying measures, along with the rationale, provide the information necessary for entities to meet the reliability objective	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question. Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-013. Request more guidance for the term "vendor" and use cases. Guidance should prompt Entities to include their definition of "vendor" in their plan(s). Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5 Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.	

The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
AECI supports NRECA's comments provided below: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	

Texas RE agrees with the proposed requirements and has the following comments.

- Question 2 above uses the term "*machine-to-machine vendor remote access*". CIP-013-1 and CIP-005-6 use the term ""system-to-system remote access". Since these are two different terms, Texas RE recommends these terms be defined or examples provided to increase clarity and to avoid multiple interpretations.
- Section 4.2.3.5 – The language, "*Each Responsible Entity shall implement develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems*." is redundant with the requirement language. Also, neither CIP-013-1 nor CIP-010-3 contain this language in the Exemptions section.
- Page 1 Section 4.1.2.2 and Page 2 Section 4.2.1.2: Texas RE noted the term "*Special Protection System"* was removed. Texas RE recommends removing this term in all CIP standards.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT is using the term *system-to-system* for consistency with other NERC Reliability Standards and definitions. Additional description has been added to the rationale section.

Section 4.2.3.5 has been maintained from approved CIP-005-5.

NERC is incorporating the approved definition of Special Protection System into the body of standards through the course of ongoing and future projects.

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes

Document Name	
Comment	
The requirement in CIP-005-5 6 Table R2.4 states that an entity must have one or more processes to determine active vendor session. We would recommend adding 'Active and Passive' to the requirement since the Measures point to passive initiation in having the vendor call or receive permission before their remote access is granted. Additional guidance on what is 'Active' and whether the monitoring session requires tracking the entire session or initiation of the session would provide more clarity to industry.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. The SDT has added clarifying details to the rationale section. This material remains with the standard following approval.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG suggest the term "vendor" be defined to exclude outsourcers that manage most aspects of a BES Cyber System. Normally they are contractually obligated to act in the Responsible Entities interests and fulfill or accommodate all compliance requirements. As such, this is a much closer relationship than is typically associated with the term "vendor". Because in many such cases they would be principle maintainer or operator of said systems would often not technically feasible to disable the outsourcer's access, remote or otherwise. Requirement 2.4 mentions ability to determine "sessions", not just "access". Requirement 2.5 is ambiguous on whether it requires the ability to disable "active sessions" as opposed to merely disabling "active accounts". Suggest replacing "access" in R2.5 with either "sessions" or "accounts" depending on what was intended or otherwise elaborating.	

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Requirement R2 Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). Depending on the responsible entity's arrangements with the vendor, outsourcer management of a Responsible Entity's BES Cyber System may not be within the scope of Parts 2.4 and 2.5. These requirement parts apply to Interactive Remote Access with a vendor and system-to-system remote access with a vendor. The SDT has clarified in the rationale section that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor. The SDT believes that contractors performing functions such as staff augmentation in a manner similar to an entity's own employee would not fall within the scope of Part 2.4.

As stated in the rationale, the objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52). The SDT believes the requirement and rationale are clear.

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski

Answer	Yes
Document Name	

Comment

GRE requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
AZPS agrees with the inclusion of Parts 2.4 and 2.5 within CIP-005-6 R2; however, requests the statement “active vendor remote access sessions” be changed to “active vendor remote connection.” A vendor may sustain an active remote connection for longer than an individual active remote access session. Thus, a revision to the language would clarify the intent of this requirement, which is to monitor any time a vendor is connecting to and accessing sensitive cyber assets remotely. Thus, AZPS encourages the SDT to consider this revision as it will better ensure that active remote connections by vendors are monitored and addressed.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes Part 2.4 and 2.5 are clear as written.	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Recommend creating a CIP-005-6 and CIP-010-3 ‘Guidance document’ similar to the one for CIP-013-1. Request that the narrative for the term 'Vendor' that is in the CIP-005-6 R2 Rationale box be added to the already Endorsed Guidance document for CIP-013-1 and to the Guidance documents for CIP-005-6 if it is created. Request that a narrative for the term 'System-to-System’ be added to the already Endorsed Guidance document for CIP-013-1 and to the Guidance documents for CIP-005-6 if it is created. Recommend removing CIP-013 R1 subparts 1.2.6 from CIP-013 since it is covered in the proposed CIP-005-6. Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5 Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the added parts (Part 2.4 and 2.5) and associated measures, and the rationale section, identify the responsible entity’s obligations and provide flexibility for the responsible entity to meet the vendor remote access reliability objectives identified in the project SAR. The rationale section remains in the standard following approval. The SDT believes they	

have fulfilled the tasks in the SAR and are not intending to develop Implementation Guidance for CIP-005-6 Requirement R2 Parts 2.4 and 2.5. Per NERC's Compliance Guidance Policy, registered entities may develop examples or approaches for complying with Reliability Standard requirements and vet them through an approved organization for ERO Enterprise endorsement consideration. The SDT has provided a description of *vendor* in the rationale section and has clarified the meaning of *system-to-system*. Rationale that is drafted during standards development remains part of the approved standard. CIP-013-1 Requirement R1 Part 1.2.6 addresses procurement processes related to vendor remote access. The proposed requirements in CIP-005-6 are operational in nature and not related to procurement. Therefore the requirements are not duplicative. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Request more guidance for the term "vendor" and use cases. If "Vendor" is not defined by NERC, the guidance should prompt Entities to include their definition of "vendor" in their plan(s). Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5	

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard.

The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
As currently written, it is ambiguous in 2.4 as to why an entity needs to "determine" vendor access, especially in conjunction with the logging, monitoring and control activities described within the measures. PJM suggests combining 2.4 and 2.5 together ("Have one or more method(s) to determine and disable active vendor remote access sessions…").	
Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT believes parts 2.4 and 2.5 describe two distinct reliability objectives which should remain separate for clarity.	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
ITC Holdings agrees with the below comment submitted by MRO's NSRF: The NSRF question the use of "…*active* vendor…" in part 2.4 and 2.5 Requirements. The word "active" could mean either "the vendor is currently allowed electronic access and is currently within a BES Cyber Asset" OR "the vendor is idle and but has electronic access to a BES Cyber Asset". The NSRF recommends that "active" be removed as this will provide clarity to applicable entities. If active sessions was the SDT thought process, please state that within the proposed part.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include: • *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;* • *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or* • *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*	

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

The definition of vendor is crucial to an entity defining and carrying out its compliance objectives for the requirements in question.

The definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-013.

Request more guidance for the term “vendor” and use cases. Guidance should prompt Entities to include their definition of “vendor” in their plan(s).

Regarding CIP-005-6, R2.4 & R2.5; NRG requests that the NERC SDT define or further clarify the meaning of “system-to-system” remote access.

NRG asserts that Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Please include a reference to FERC Order 829 for Parts 2.4 and 2.5.

Please consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

Requirement R2 Parts 2.4 and 2.5 address controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to “user-initiated access by a person”, the SDT included system-to-system remote access with a vendor(s) in the

requirement to meet the directive in Order No. 829 (P. 45). The SDT has clarified in rationale that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Does system to system remote access include “read-only” access or all forms of external access from vendors?	

Likes 0	
Dislikes 0	
Response. Thank you for your comments. Taken together, *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all remote access sessions with vendors. This includes 'read-only' access.	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has added clarification to the Rationale section. The rationale remains in the standard following approval.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

The proposed CIP-005-6 uses vendor. Definition of vendor is not a NERC defined term. USI believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that Entities include their definition of "vendor" in their plan(s). The SDT should consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response. Thank you for your comment. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. The SDT does not believe a CIP Exceptional Circumstance would prevent an entity from having methods for determining active remote access sessions or disabling remote access sessions.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
As stated, this requirement seems to start with the base assumption that the Registered Entity allows vendors to have Remote Access to the Registered Entity's BES Cyber Assets with External Routable Connectivity (ERC), and therefore must implement a method to detect active vendor remote access session and have a method for disabling vendor access. Many Registered Entities do not allow vendors to have Remote Access to substation medium BES Cyber Assets. Would this relieve such REs from having to then develop a method to detect and disable active vendor remote access session and would documentation demonstrating that Vendor Remote Access was not allowed be sufficient?	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the rationale section. The rationale remains in the standard following approval.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA requests that the SDT clarify in the requirements and GTB that applicable entities that do not allow Remote Access, do not have to create a process for Remote Access or terminating Remote Access.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. It is not the intent of the SDT to require entities to have documented processes for remote access if the entity does not allow remote access. The SDT has added clarification to the rationale section. The rationale remains in the standard following approval.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
The definition of “vendor” is important for defining and carrying out its compliance objectives for the requirements parts 2.4 and 2.5. The drafting team should add a part of one or both requirements to include a specific definition of vendor to support the related compliance procedures and evidence required of an entity.	

For Part 2.4, it is not clear if the requirement applies to contractors and service vendors that are provided authorized access under CIP-004. Additionally, more information is needed on the meaning of "active". Most of this is captured in logs after the fact. Does the drafting team intend for "active" to imply real-time information? Please clarify if the requirement only applies to a connection from the vendor directly to a system within the ESP or does it apply to connections from a vendor to a system outside the ESP that updates one inside the ESP. For Part 2.5, Oncor would like clarification of the action, or examples, for when access should be disabled.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.

Part 2.4 does not exclude contractors and service vendors that are provided access under CIP-004. Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). Depending on the responsible entity's arrangements, contractor and/or vendor management of a Responsible Entity's BES Cyber System may not be within the scope of Parts 2.4 and 2.5. These requirement parts apply to Interactive Remote Access with a vendor and system-to-system remote access with a vendor. The SDT has clarified in rationale that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.

The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include:

- *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;*

- *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or*
- *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*

CIP-005-6 Requirement R1 Part 1.5 could provide a mechanism for Responsible Entities to determine when a response to suspicious activity in a vendor remote access session may be warranted. Part 1.5 requires Responsible Entities to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Detections associated with this requirement could determine when a responsible entity should disable vendor remote access.

Lona Calderon - Salt River Project - 1,3,5,6 – WECC	
Answer	Yes
Document Name	
Comment	

SRP agrees with R2 Part 2.4 but requests clarification of the term “determining.”

SRP generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “…is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. SRP requests changing the language to “upon detected unauthorized activity.”

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the subjective term 'rapidly'. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions.

Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	

Request to defined the scope of the requirements "for new contracts only"

With no defined scope, if the standard become effective in same time of the standard CIP-013-1, no terms will existed beetween entities and vendor in effective contracts. How the entities will comply to requirements ?

Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.

Request more guidance for the term "active vendor remote access sessions" and use cases. Guidance should prompt Entities to include their definition of "vendor" in their plan(s).

Guideline & Technical Basis for R2 should be included in this update. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Include reference to FERC Order 829 for Parts 2.4 and 2.5

Consider adding a CIP Exceptional Circumstance clause to R2 Parts 2.4 and 2.5

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT does not agree with limiting the scope to new contracts. The SDT believes responsible entities can and should meet the requirements upon implementation of the standard. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. *Active* sessions refers to remote access sessions with vendors that are taking place on the responsible entity's system at any point in time. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See atttached comments.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard.	

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the term 'rapidly'. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions. The SDT included reference to FERC Order No. 829 in the rationale section for R2. This and other information in the rationale will become part of the supplemental material following NERC Board adoption of the proposed standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro sees value in adding the machine to machine vendor remote access component.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes

Document Name	
Comment	
AE agrees with R2 Part 2.4 but requests clarification of the term “determining.” AE generally agrees with Proposed R2 Part 2.5, but requests revisions to the rationale for R2. The last sentence of paragraph 2 states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. AE requests changing the language to “upon detected unauthorized activity.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the subjective term ‘rapidly’. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

SMUD agrees with R2 Part 2.4 but requests clarification of the term “determining.” SMUD generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. SMUD requests changing the language to “upon detected unauthorized activity.” Clarification or formal definition of the term ‘vendor’ should be considered. ICCP and DNP3 traffic is routine system-to-system remote access between utilities, Operation and Maintenance vendors and other partners to provide reliability, without the term ‘vendor’ clarified, these protocols may fall into scope unnecessarily.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT has revised the rationale and removed the subjective term ‘rapidly’. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions. Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). As stated in the rationale, NERC registered entities are not considered vendors within the scope of the requirements. The SDT did not intend to exclude certain remote access on the basis of a responsible entity considering the remote access to be ‘routine’.	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	

Comment
PRPA agrees with R2 Part 2.4 but requests clarification of the term “determining.” PRPA generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective “is for entities to have the ability to rapidly disable active remote access sessions…” The Responsible Entity may not have the capability to disable access during an “active” remote access session. PRPA requests changing the language to “upon detected unauthorized activity.”

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective.

The SDT has revised the rationale and removed the subjective term ‘rapidly’. The objective of part 2.5 is for entities to have the ability to disable active remote access sessions.

Anthony Jablonski - ReliabilityFirst - 10	
Answer	Yes
Document Name	

Comment
ReliabilityFirst agrees the changes to CIP-005-6 address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 to develop a new or modified standard to address “supply chain risk management for industrial control system hardware, software, and

computing and networking services associated with bulk electric system operations." ReliabilityFirst offers the following specific comments for consideration.

1. Requirement R2 Part 2.3
    i. To be consistent with Parts 2.1 and 2.2 in the Standard, ReliabilityFirst offers the following modifications for consideration:
        a. [For all Interactive Remote Access sessions, require] multi-factor authentication.
2. Requirement R2 Part 2.4
    i. ReliabilityFirst believes more context should be placed around the term "determining". ReliabilityFirst offers the following modifications for consideration:
        a. Have one or more method(s) for [authorizing, monitoring, and logging] active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes part 2.3 is clear as written.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The word *determining* in this context describes actions that the responsible entity could take to meet the objective. The SDT believes the suggested wording could create overlapping obligations with some approved CIP requirements. The SDT prefers the drafted wording because it provides responsible entities with more flexibility to meet the objective.

Allan Long - Memphis Light, Gas and Water Division - 1

Answer	Yes
Document Name	
Comment	
Because the term "vendor" is not a NERC-defined term, the SDT should provide guidance regarding its use. A "CIP Exceptional Circumstance" clause should be added to R2, Parts 2.4 and 2.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. The SDT discussed the suggestion to consider adding CIP Exceptional Circumstance and did not believe this was necessary for reliability. Responsible entities can be expected to meet the obligations in Part 2.4 and 2.5.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
A definition of “vendor” is necessary. This should be interpreted as any third-party that initiates a remote access session. Not every third-party is necessarily considered a “vendor” based on generally accepted definitions. With respect to the proposed Requirement 2 Part 2.4, additional details need to be provided on the expectations of “determining active vendor remote access sessions”. Two of the proposed measures state, “Methods for monitoring activity (e.g. connection tables or rule hit	

counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; **or** Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access." The former will be difficult to actively monitor for remote access. Remote access can be monitored, but this activity is too resource intensive to monitor in real-time. If it is necessary to actively monitor remote access in real-time then additional guidance is necessary. The latter is easily implemented. It is uncertain whether this requirement is expecting constant monitoring during the remote access session or just controlling access and logging the access. A more detailed expectation on the use of the reference tools is necessary.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided a description of *vendor* in the rationale section. Rationale that is drafted during standards development remains part of the approved standard. Some remote access, such as between NERC Registered Entities, is not considered in scope for Parts 2.4 and 2.5. The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. However, a responsible entity could choose to monitor vendor remote access sessions in real time as a way to meet its obligation in Part 2.4.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
As in Question 1, regarding the use of the term “vendor,” as described in the “Rationale for Requirement R2” section of CIP-005-6: the SDT may want to clarify that staff augmentation contractors are not considered to be “vendors” in the context of the standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. Parts 2.4 and 2.5 are intended to mitigate risks of a compromise at a vendor from traversing over a network connection and impacting BES Cyber Systems (Order No. 829 P. 52). Depending on the responsible entity’s arrangements, staff augmentation contractors may not be within the scope of Parts 2.4 and 2.5. These requirement parts apply to Interactive Remote Access with a vendor and system-to-system remote access with a vendor.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	

Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
We request clarification on whether “system-to-system” access applies to access that is “one-way” where the remote end conducts only monitoring activity and no control is possible, or whether the SDT intent is that any system-to-system access be included. We would suggest that the SDT add verbiage to the Guidelines and Technical Basis making the distinction for each type of “active vendor remote access sessions” that are included in this requirement (Interactive Remote Access, system-to-system remote access with control, and/or system-to-system remote access for monitoring only). Another suggestion would be to create a formal NERC definition of system-to-system access.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Parts 1.2.6 addresses controls for remote access with vendors. Because Interactive Remote Access as defined in the NERC glossary is limited to “user-initiated access by a person”, the SDT included system-to-system remote access with a vendor(s) in the requirement to meet the directive in Order No. 829 (P. 45). The controls specified in Part 1.2.6 cover all remote access with vendors, which includes one-way remote access. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (i) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.

Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	

Document Name	
Comment	
Please clarify definition of system-system communications	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has clarified in rationale that the phrase *active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access)* covers all active remote access sessions with vendors. System to system remote access is any remote access that: (i) is permitted by the Responsible Entity according to Requirement R1 Part 1.3, (ii) is not IRA, and (iii) occurs between the Responsible Entity and a vendor.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	

Document Name	
Comment	
The NSRF question the use of "…*active* vendor…" in part 2.4 and 2.5 Requirements. The word "active" could mean either "the vendor is currently allowed electronic access and is currently within a BES Cyber Asset" OR "the vendor is idle and but has electronic access to a BES Cyber Asset". The NSRF recommends that "active" be removed as this will provide clarity to applicable entities. If active sessions was the SDT thought process, please state that within the proposed part.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT's intent for Requirement R2 Part 2.4 is for entities to have the ability to determine all remote access sessions with vendors that are taking place on their system at any point in time. Meeting this objective does not require monitoring of remote access sessions in real time. The examples of evidence included in the Measures for Part 2.4 indicate that this method does not require monitoring of individual remote access sessions with a vendor in real time. Examples listed in the measure include:

- *Methods for accessing logged or monitoring information to determine active vendor remote access sessions;*
- *Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or*
- *Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.*

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Disagree with the revisions on CIP-010-3, would like to see guideline language of verifying once be moved to the requirement/measure	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that verification checks are not duplicated for each installation. The SDT believes the requirement and measures are worded to provide responsible entities flexibility to use this approach.	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	No
Document Name	
Comment	
Need additional information regarding how to verify integrity of software.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has added information to the guidelines section.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	No
Document Name	
Comment	
Duke Energy requests additional guidance as to what constitutes acceptable verification of integrity as required by R1.6.2. The measure indicates that a change request record could demonstrate that source identity and integrity verification took place, but doesn't go into further detail as to what an acceptable check into source identity and software would be. Is there specific language that should be stated in the change request record that would clearly state the verification took place? More guidance on this aspect is requested. Also, Duke Energy requests that the Note under Applicable Systems in Part 1.6 should remain there once the standard is approved. The Note provides valuable details as to the true scope of the Requirement, and aids entities in knowing what will be the compliance expectation.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has added information to the guidelines section. The note remains in the Part 1.6 when the standard is approved.	
Timothy Reyher - Eversource Energy - 5	
Answer	No

Document Name	
Comment	

Comments:

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions:

How does one prove that a method is not available?

What is the line between available/unavailable? How far do you have to go?

We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Additional examples are included.

For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1.

An entity could demonstrate that a method to verify integrity is not available by providing documentation from the software source that shows the method to verify integrity is not provided, could provide evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.

The SDT included 'when a method to do so is available' to provide flexibility necessary to prevent disruption of an entity's software update and patch management processes. Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing "when the method to do so is available to the Responsible Entity from the software source" to "when the vendor supplied method to do so is available to Responsible Entity". Otherwise the "method to do so" is ambiguous and leaves the following questions:

How does one prove that a method is not available? What is the line between available/unavailable? How far do you have to go? We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Additional examples are included. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. An entity could demonstrate that a method to verify integrity is not available by providing documentation from the software source that shows the method to verify integrity is not provided, could provide evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT included 'when a method to do so is available' to provide flexibility necessary to prevent disruption of an entity's software update and patch management processes. Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	

Comment	
The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation.	
IESO	
Answer	No
Document Name	
Comment	
The IESO is concerned with two aspects of CIP-010-3 Requirement R1 Part 1.6: 1. The phrase “when the method to do so is available to the Responsible Entity from the software source” will be difficult to audit and difficult for the Responsible Entity to confirm as it is hard to prove a negative. The IESO suggest that verification of software source and integrity can take many different forms and is a sufficiently common practice that this phrase is not required. To take into consideration legacy software, the IESO suggest the wording be adjusted, to reflect FERC intentions that the requirements are forward looking, by replacing the phrase “and when the method to do so is available to the Responsible Entity from the software source” with “and, at a minimum, for the portion of the software that has changed:”	

2. There appears to be inconsistency between the requirement and the Guidelines.

The requirement states “For 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”.

The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit.

Therefor the IESO suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IESO suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT believes the phrase ‘when a method to do so is available’ provides responsible entities with necessary flexibility to perform configuration management obligations. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity’s software update and patch management processes.

The SDT has removed unclear statements from the guidelines section and added additional guidance.

The SDT revised the measure for Part 1.6 to provide an example of evidence to support automated solutions.

William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
See attached integrated comments. (Comment at end of document)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
To avoid an interpretation of this requirement that may be overly burdensome, ERCOT suggests the following clarifications to the language in the requirement and measure of CIP-010-3 R1 Part 1.6. This would ensure a more holistic and less prescriptive approach to changes that deviate from the baseline. In the first sentence of Requirement R1.6, revise "For a change that deviates" to "Where technically feasible, for changes that deviate…" Revise the R1.6 Measure to read "An example of evidence may include, but is not limited to, a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed during the baseline change, *or a process which documents the mechanisms in place that would automatically ensure the authenticity and integrity of the software."*	
Likes 0	

Dislikes 0	
Response. Thank you for your comments. The SDT included the wording 'when a method to do so is available', which is intended to cover issues that would include technical feasibility. The SDT has made the suggested change to the measure for Part 1.6.	
Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 "Note:" within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; "CHPD has concerns about language related to procurement contracts, in particular use of master agreements,	

piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.” CIP-010 R1.6 – Applicable System Note *“Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 “Note:” within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; “CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to “contracts” and most references to “procurement” be struck from CIP-013.” CIP-010 R1.6 – Applicable System Note	

"Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract."	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 "Note:" within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; "CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013." CIP-010 R1.6 – Applicable System Note *"Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract."*	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD believes the R1.6 "Note:" within the Applicable Systems section (shown below) must be removed to be consistent with the CHPD response to question 1; "CHPD has concerns about language related to procurement contracts, in particular use of master agreements, piggyback agreements, and evergreen agreements. To address these concerns and position CIP-013 as a performance based Standard, CHPD recommends that all references to "contracts" and most references to "procurement" be struck from CIP-013." CIP-010 R1.6 – Applicable System Note *"Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract."*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the note is consistent with the forward-looking nature of Order No. 829. The SDT also believes Part 1.6 is performance-based.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	No
Document Name	

Comment
The language should make clear that verification is required for the software intake process, but not for each subsequent installation. We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions: - How does one prove that a method is not available? - What is the line between available/unavailable? How far do you have to go? We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.
Likes 0
Dislikes 0
Response. Thank you for your comments. The SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Part 1.6 provides responsible entities with flexibility to meet the reliability objective. A responsible entity could use a verification method that is provided by the vendor, or another method that is available. Techniques described in the guidelines and technical basis section are not limited to those provided by the software’s vendor. An entity could demonstrate that a method to perform verification is not available by providing documentation from the software source, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT included ‘when a method to do so is available’ to provide flexibility necessary to prevent disruption of an entity’s software update and patch management processes. Part 1.6 does not impact an entity’s ability and obligation to meet CIP-007 R2.
Shawn Abrams - Santee Cooper - 1

Answer	No
Document Name	
Comment	

Need clarification about how the addition of R1.6 applies only to BES Cyber Systems that are newly implemented and thus did not previously have a baseline and as such do not have an existing baseline to deviate from. Please clarify that this is for new BES Cyber Systems to avoid confusion and challenges during an aduit.

Need some additional examples of what constitutes evidence to meet compliance to this standard. Some systems are not connected to the internet purposefully and as such patches are installed utilizing a CD/DVD provided by the vendor. What would constitute appropriate evidence for a case such as this?

This requirement is not clear whether an entity has to duplicate efforts for every case for which such verification has to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that an entity can verify once and apply to many assets.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline is not in scope for Part 1.6. Baseline changes to the responsible entity’s high impact and medium impact BES Cyber Systems after the effective date of proposed CIP-010-3 are in scope (i.e., Part 1.6 is not limited to new BES Cyber Systems.)

SDT has provided additional technical considerations and examples in the guidance section, and revised the measure. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation.

Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
Since the intent of CIP-010-3 R1.6 is a proactive verification of software integrity, R1.6 should focus on a single verification prior to introducing vendor software into the production environment. The current language of R1.6 utilizes a retroactive focus via baseline deviations. Please see the suggested wording - "Prior to introducing software not resident in baseline items (per 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."	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised Part 1.6 to clarify that the verifications are to be performed prior to the baseline change.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	

Proposed Requirement R1 Part 1.6 appears to require verification of identity and integrity of applicable changes to the baseline. However, the measure for this requirement gives an example of having a process, e.g., a change request record, instead of a specific example of verification. Can the team clarify the measure for this Requirement as an entity can have a change ticket process that merely requires the user to click a button that states that the software has been verified, however, if the team believes proof of such check, such as a screenshot of the vendor site, is required, please state such as an example. Additionally, the example of evidence does not demonstrate how a software source or the software integrity is verified. An internal change ticket is not a verification of the software source. If they are going to push for source verification then modify CIP-007 R2.1 to include it. Specifically, what is expected as evidence -- a hash, screenshot, attestation, digital signature?	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has provided additional guidance and examples in the guidelines and technical basis section.	
Anthony Jablonski - ReliabilityFirst - 10	
Answer	No
Document Name	
Comment	
Even though ReliabilityFirst believes the changes to CIP-010-3 draft standard address directives from Federal Energy Regulatory Commission (FERC) Order No. 829 and is a positive step in addressing cyber supply chain management, ReliabilityFirst Abstains mainly due to Requirement R1 missing Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs). ReliabilityFirst offers the following specific comments for consideration. 1. Requirement R1 Part 1.6 2.	

i. ReliabilityFirst believes the "Applicable Systems" under Requirement R1 Part 1.6 should be consistent with "Applicable Systems" under parts 1.1, since sub-parts (Part 1.1.1, 1.1.2, & 1.1.5) are called out under the "Requirements" section for Part 1.6. EACMs and PACS are critical cyber assets that control access and monitoring into the entities' ESPs and PSPs and should follow the Supply Chain standard/requirements as do the High and Medium Impact Cyber Systems. As for the PCAs, if they are compromised due to a vulnerability in the vendors supplied hardware or software, they can possibly affect high and medium impact BES Cyber Systems. ReliabilityFirst offers the following modifications for consideration for the "Applicable Systems" column in Requirement R1 Part 1.6:

   a. High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA

   b. Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA

3. Requirement R1 Part 1.6.3 (new sub-part)

   i. ReliabilityFirst believes a new sub-part 1.6.3 should be added to address the verification of the baseline configuration. ReliabilityFirst offers the following new sub-part 1.6.3 for consideration:

      a. Verify the deviations from the baseline configuration.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT believes that Part 1.6 provides the intended reliability benefit, which applies to "industrial control system hardware, software, and services associated with bulk electric system operations" as specified in Order No. 829 (P. 43). The SDT believes entities should have flexibility to determine supply chain cyber security risk management controls for other cyber assets, including EACMS, PACS, and PCAs. The SDT believes this is an appropriate risk-based approach that allows entities to focus resources where they provide the most reliability benefit.

SDT believes there is reliability benefit to addressing the software integrity for changes from baseline configuration and that the requirement meets the directives in Order No. 829. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Verification of the integrity of the baseline configuration is not in scope.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro does not agree with value-add of this standard requirement. Under current CIP requirements, CIP controls around testing of changes and ongoing monitoring of systems would mitigate any risk associated with software identity or integrity.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (Order No. 829 P. 49). The SDT agrees that other entity processes help mitigate risk. However, Part 1.6 is responsive to the project SAR and provides reliability benefit by addressing some verifications that are not covered under other standards.	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	

Ther is nothing wrong with the concept of the requiment however the language of the requirement is not supportable. The term available could me technically available, procedurally available, contracturaly available, freely available (no support purchase required). As written this requirement by its nature will be implemented and assessed drastically differently by different Responsible Entities. One could argue that only if all the available methods listed above exist in unison is software actually available.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. SDT has provided additional information in the guidance section. *Available from the software source* is not intended to be limited to contract terms. The SDT believes this wording is necessary to provide entities with flexibility and avoid disrupting software update and patch management processes in some situations.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
There are auditing challenges around the phrase “when the method to do so is available to the Responsible Entity from the software source” as it is hard to prove a negative. Oncor believes that verification of software source and integrity can take many forms. To take into consideration legacy software, Oncor believes the wording should be adjusted, to reflect FERC intentions that the requirements are forward looking, by replacing the phrase *“and when the method to do so is available to the Responsible Entity from the software source”* with *“and, at a minimum, for the portion of the software that has changed:”* Second, the proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). We offer a recommendation on the language, *“Document and implement a software source management process to address source identity*	

verification and media integrity controls on the software repository used for changes that deviate from the existing baseline configuration associated with items in parts 1.1.1, 1.1.2, and 1.1.5." *This process must include steps:* *• To verify the identity of the software source when the method to do so is available; and* *• To verify the integrity of the software obtained when the method to do so is available.* *Evidence may include verification of identity of the software source and integrity of the software was performed for repository updates."*	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. An entity could demonstrate that a method to perform verifications is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). The SDT does not believe the replacement phrase for 'when a method to do so…" is necessary or provides additional clarity. Performing software verifications as part of establishing the baseline is not in scope for Part 1.6. SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. The SDT believes this addresses concerns with duplicating efforts.	
Don Schmit - Nebraska Public Power District - 5	
Answer	No

Document Name	
Comment	
NPPD supports the comments of the MRO NSRF, in addition: Auditors will have too much discretion as to what is or is not enough for a validation check of each vendor, which will lead to inconsistencies across the NERC RE footprint. It is up to entities to document what the vendor is willing to do and hope the auditors agree it is enough to continue doing business with the vendor. Also, the language of the requirement says "…when the method to do so is available…". If a vendor does not have a method to do so, but does in the next year or so, the entity may have a possible violation if it did not realize there was a change in the vendor's available methods. This would force entities to periodically check to see if the vendor capabilities have changed. What is the period that would not make this a violation? The requirement is very vague.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes Part 1.6 addresses the reliability objective for software verification contained in the project SAR and provides responsible entities with the flexibility necessary to meet the obligation. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity's software update and patch management processes. SDT has added guidance in the technical guidelines section to support responsible entities in adding this objective to their configuration change management processes.	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	

As currently written, "verify the identity" is too vague. PJM suggests adding examples of "identify" into the measure. PJM also suggests removing the word "software" from 1.6.1 and 1.6.2 as it is already stated within parts 1.1.1, 1.1.2 and 1.1.5 (firmware should be within the scope of 1.6).	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT added guidance in the guidelines section of the standard. The scope of Part 1.6 includes any changes (software or firmware) in 1.1.1, 1.1.2, and 1.1.5.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many. Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence. We support these changes, but requests clarification about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.	
Likes 0	

Dislikes 0	

Response. Thank you for your comments.

The SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Technical considerations and examples associated with Part 1.6.1 and Part 1.6.2 are included.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., implementing a new BES Cyber System) is not in scope for Part 1.6.

Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	

Comment

Request clarification on how an Entity can verify the 'integrity and authenticity' one time and then be able to install on multiple devices.

Recommend removing CIP-013 R1 subparts 1.2.5 from CIP-013 since it is covered in the proposed CIP-010-3

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. Request guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

VSL does not cover the failure to implement the process. Does not include all of the combinations.

Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence

We suggest rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” is ambiguous and leaves the following questions: How does one prove that a method is not available? What is the line between available/unavailable? How far do you have to go? We are concerned with double jeopardy potential with CIP-007 R2. We feel that if it is impossible to validate the source or verify authenticity of the patch itself we would not consider that patch to be available.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

The SDT added guidance to support use of software repositories so that integrity checks are not duplicated for each installation. Technical considerations and examples associated with Part 1.6.1 and Part 1.6.2 are included.

CIP-013-1 Requirement R1 Part 1.2.5 addresses procurement processes related to software verification. The proposed requirement in CIP-010-3 is operational in nature and not related to procurement. Therefore the CIP-013 requirement is not duplicative of the CIP-010-3 requirement. The SDT believes both operational controls and procurement related processes provide reliability benefit and are needed to address the directives in Order No. 829.

For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1.

Part 1.6 provides responsible entities with flexibility to meet the reliability objective. A responsible entity could use a verification method that is provided by the vendor, or another method that is available. Techniques described in the guidelines and technical basis section are not limited to those provided by the software’s vendor. An entity could demonstrate that a method to perform verification is not

available by providing documentation from the software source, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT included 'when a method to do so is available' to provide flexibility necessary to prevent disruption of an entity's software update and patch management processes. Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
To ensure that resources are appropriately focused on changes to be applied, AZPS recommends clarifying that verification should be completed "prior to application of a change." Such a clarification will signal to entities that verification only needs to be performed where a change will be applied and avoid circumstances where a change is being evaluated for application and verification occurs, but the change is not applied. Under the current obligation, it is likely that verifications and associated evidence would be prepared regardless of whether the change is or is not applied and would therefore result in the dedication of resources to efforts that would have no benefit to reliability or security. Additionally, AZPS requests clarification regarding the continued need for verification evidence where such is not available from the vendor. Specifically, AZPS notes that, where a vendor's policy does not provide the necessary evidence associated with verification, this Requirement may frequently represent null evidence for areas where items are reviewed each time a change occurs, but no data is available due to the vendor's policies. Such efforts would be redundant and of little or no value to security and reliability.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised Part 1.6 to clarify that the verifications are to be performed prior to the baseline change.	

The SDT believes Part 1.6 and its associated measure provide the responsible entity with flexibility to develop configuration change management processes and evidence that minimize redundant efforts. Specific questions pertaining to auditing and compliance are not in scope for the SDT.	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Add language to address CIP Exceptional Circumstances.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT discussed the suggestion to add CIP Exceptional Circumstance and did not believe this was necessary for reliability. The SDT believes the steps for verifications, when methods are available, can be implemented in emergent and non-emergent scenarios. Furthermore, responsible entities are not obligated to perform verifications when a method to perform the verifications is not available.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	

Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE and NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
OPG suggest that 1.6.1 state "Verify the software originated from the vendor's official source(s)". In the current text, even if a source has an "identity", it should also state the "identity" is the one that is expected. Similarly we can change the word "identity" with "correct identity" in R1 Part 1.6.1.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. SDT agrees that verifying identity of source means that the software is being obtained from the correct source. The SDT believes the additional information provided in the guidance section clarify the intent.	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
By adding the "when the method to do so is available to the Entity from the software source" does this require the entity to document and detail what method is available of not available? How does that entity prove and document this condition? Does the entity have to document and prove that it was tested and verified for software integrity and authenticity? If so, what are those requirements, documentation, testing environment required and timeline for testing the software?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	

AECI supports NRECA's comments provided below: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Victor Garzon - El Paso Electric Company - 5	

Answer	Yes
Document Name	
Comment	

EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated:

For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without **verification that the component has been digitally signed** to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides **examples of controls for addressing the Commission's directive regarding this first objective. Other security controls also could meet this objective.** Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.

Likes 0	

Dislikes 0	
Response. Thank you for your comment. Consistent with other NERC Reliability Standards, the suggested clarifications are more appropriately addressed in the guidelines section of the standard. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	

EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated:

For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without **verification that the component has been digitally signed** to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides **examples of controls for addressing the Commission's directive regarding this first objective. Other security controls also could meet this objective.** Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Consistent with other NERC Reliability Standards, the suggested clarifications are more appropriately addressed in the guidelines section of the standard. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
EPE understands the need for software integrity and authenticity; however, the proposed wording of the standard is not sufficiently clear with respect to the action/conduct being sought by the Registered Entity in order to achieve compliance. In Order No. 829, FERC offered clarity that the proposed requirement does not capture. There, FERC stated: *For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and components should be tested and verified using controls such as digital signatures and obtaining software directly from the developer. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without verification that the component has been digitally signed to ensure that hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing the*	

Commission's directive regarding this first objective. Other security controls also could meet this objective. Order No 829 at P 50 (emphasis added).

Requirement 1.6 should be adjusted to provide the type of clarity FERC provided in the Order. An additional sentence or parenthetical should be included within the requirement, to read ("Verification that a patch or other software component has been digitally signed is one way to meet this requirement; other security controls could also meet this requirement, such as having the vendor state in writing that it will verify the integrity and authenticity of all software, including patches, in advance of releasing it to the Registered Entity during the life of its service contract with the Registered Entity").

The addition of such language *in the requirement itself* is consistent with the feedback offered by NERC Staff in recent months, and would eliminate the false impression that would otherwise be given that a Registered Entity must secure a verification letter from its software vendor each and every single time it seeks to download a patch. For example, during the NERC webinar held on May 18, 2017, examples were provided to the attendees on information that would be considered sufficient evidence to fulfill this requirement, and such examples included a letter from the vendor indicating that the vendor is verifying integrity and authenticity of its software before releasing its software (including patches) to its clients.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. Consistent with other NERC Reliability Standards, the suggested clarifications are more appropriately addressed in the guidelines section of the standard. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company

Answer	Yes
Document Name	

Comment

Additional examples of acceptable evidence would be helpful under the Measures column of the requirement.

Change the statement in the Guidelines and Technical Basis, Section Software Integrity and Authenticity, paragraph 1, third sentence: "The intent of the SDT is to provide controls for verifying the baseline elements that are *updated* by vendors." to say "… *provided* by vendors." Additional clarity is needed regarding the following in the Guidelines and Technical Basis: "It is not the intent of the SDT to require a verification of each source *or software update at the time it is obtained*. It is sufficient to *establish the reliable source and software update once*. This will allow automated solutions to be implemented to obtain frequent updates such as patches." This is confusing because saying "each source or software update" is not required to be validated at the time it is obtained could be interpreted to mean continuous patch updates provided by a single vendor are only required to be verified once for the lifetime of the supply of patches from that vendor. Additional examples of acceptable methods and evidence are needed in the Guidelines and Technical Basis for performing software integrity and authenticity. For example – Consider having the measures for R1.6 be similar to R1.1.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT revised the Measure for Part 1.6 to more clearly include automated processes for verifications. The SDT has added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard. The SDT believes the suggested change of *updated* to *provided* could confuse some responsible entities because the requirement applies to baseline changes only; therefore the SDT does not support the wording change. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. In doing so, the SDT removed ambiguous information from the guidelines section.
Teresa Cantwell - Lower Colorado River Authority - 1

Answer	Yes
Document Name	
Comment	
Disagree with the revisions on CIP-010-3. We would like to see guideline language of verifying once be moved to the requirement/measure.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance to support use of software repositories so that verification checks are not duplicated for each installation. The SDT believes the requirement and measures are worded to provide responsible entities flexibility to use this approach.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	

Comment	
We request clarification on the timing of requirement 1.6; specifically, on whether 1.6 must be completed before being placed in operation on a BES Cyber System. This distinction was made in the previous draft ("one or more documented process(es) for verifying the integrity and authenticity of the following software and firmware before being placed in operation on high and medium impact BES Cyber Systems"). Under the current language, it appears sub-requirement 1.6 could be done before or after the software is placed on a BES Cyber System. We suggest the SDT add a timeframe similar to the other CIP-010 R1 sub-requirements. For example, 1.3 states "within 30 days" while 1.4.1 states "prior to the change". Additionally, we request adding 1.1.3 (any custom software installed) to 1.6, as custom software could be internally or externally provided, and needs to be verified for integrity and authenticity.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised Part 1.6 to clarify that the verifications are to be performed prior to the baseline change.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	

Answer	Yes
Document Name	
Comment	
No issues from an SCRM perspective. Part 1.6 is generic and can be considered a good idea for all changes from baseline configurations described in Parts 1.1.1, 1.1.2, and 1.1.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	

Comment
Need to emphasize the phrase “and when the method to do so is available to the Responsible Entity for the software source”. Since this is a non-prescriptive requirement it is expected that we will be demonstrating compliance by implementing the plan(s) required in CIP-013. Since it may not be possible to hold the software resource directly responsible it is expected that the demonstration of “best effort” will be sufficient and not subject to interpretation by the Compliance Enforcement Authority. Recommend providing more examples of suitable evidence that should be gathered to verify identity and integrity. The Measure as currently written is too vague.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT has added details to the guidelines section to provide technical considerations and examples that improve the clarity of the standard.

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	

Comment
We support APPA's submitted comments, including: This requirement would possibly involve entitites duplicating effort for every case for which such verification had to be undertaken. More examples of evidence should be provided. Clarification is needed about how new R1.6 applies to entirely new BES Cyber Systems.

Likes 0	

Dislikes 0	

Response. Thank you for your comment.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

PRPA agrees this requirement belongs in CIP-010 R1. PRPA generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- PRPA recommends the Guidelines and Technical Basis section is updated to reflect current information.
    - The requirement states "For 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…," indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a

verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

- PRPA also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, PRPA requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While PRPA supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written.

An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
The Guidelines and Technical Basis of CIP-010-3 states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” CenterPoint Energy recommends incorporating this concept in the R2 requirement language in order to clarify that integrity and authenticity do not need to be verified for every source or software update, and that the download once and install on many approach is acceptable if the integrity and authenticity of the downloaded software are validated. CenterPoint Energy recommends adding the following language to Requirement R2: Upon validation of the integrity and authenticity of software, a Responsible Entity does not need to verify the integrity and authenticity for subsequent updates of such software.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT is addressing this concern by adding guidance to the guidelines section that supports use of software repositories so that integrity checks are not duplicated for each installation.
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino

Answer	Yes
Document Name	

Comment

SMUD agrees this requirement belongs in CIP-010 R1. SMUD generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- SMUD recommends the Guidelines and Technical Basis section is updated to reflect current information.
    -
        - The requirement states “For 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…,” indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

- SMUD also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, SMUD requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While SMUD supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

•

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written.

An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.

Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	

AE agrees this requirement belongs in CIP-010 R1 and generally agrees with Proposed R1 Part 1.6, but request the SDT address the following items:

AE recommends the Guidelines and Technical Basis section be updated to reflect current information.

The requirement states "For 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…," indicating the authenticity and integrity of the specified parts must be verified each time a baseline changes for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to occur (e.g., in the cases of multiple installations of software across many applicable Cyber Assets). This requirement does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe the existing statement in the GTB provides clarity on this issue and request it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

o AE also recommends rewording the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work. o There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system. o Additional examples of acceptable measures should to be listed. Additionally, AE requests examples of acceptable evidence when there is no method available to verify the identity of the software source. While AE supports these changes, clarification is required about how R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS newly implemented and which have no previous baseline, and thus do not have an existing baseline from which a change can occur. We expect R1.6 is intended to apply to new BCS as well as to existing BCS but, as written, the requirement does not. Please clarify to avoid implementation confusion and audit challenges.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.	

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body

Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment
See attached comments

Likes 0	
Dislikes 0	

Response. Thank you for your comments. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation.

Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Request to defined the scope of the requirements "for new contracts only" With no defined scope, if the standard become effective in same time of the standard CIP-013-1, no terms will existed beetween entities and vendor for effective contracts. How the entities will be conformed to requirements ? The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. VSL does not cover the failure to implement the process. Does not include all of the combinations. Concerns with 1.6.1 and 1.6.2 as written --- how to provide evidence? Request more examples of evidence.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

The SDT does not agree with limiting the scope to new contracts. The SDT believes responsible entities can and should meet the requirements upon implementation of the standard. SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1.

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP agrees this requirement belongs in CIP-010 R1. SRP generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- SRP recommends the Guidelines and Technical Basis section is updated to reflect current information.
    - The requirement states “For 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…,” indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present

an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

- SRP also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.

- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed. Additionally, SRP requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While SRP supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible

entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. An entity could demonstrate that a method is not available by providing documentation from the software source that shows methods are not provided, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is "intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System" (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	

Comment	
NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: "For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer." This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
N&ST believes the "if you can, you must" qualifying language in this proposed requirement part should be added to at least some parts of CIP-013 R1 and R2.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT does not believe that it is necessary to include this phrase in CIP-013-1 Requirement R1 Part 1.2. because CIP-013-1 addresses the responsible entity's procurement processes. CIP-013 does not impose obligations on vendors, nor does it obligate the responsible entity to specific terms or conditions in a contract.	
David Rivera - New York Power Authority - 3	

Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
The NSRF has the same comment from CIP-013-1 R1: CIP-010-3 R1.6 is troublesome as well. Entities typically use update or proxy servers to discover and identify applicable security patches. For example, we use Windows Update Server Services to identify patches and roll them out once testing and approvals are complete. Do we need to check the check sums of the identified patches or can we trust that the update servers are authenticating the software?	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT has revised the measure for Part 1.6 to include evidence of meeting the requirement using automated update mechanisms. The SDT has also added details to the guidelines section to provide technical considerations and examples that will improve the clarity of the standard.	

Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."

USI has concerns with R 1.6.1 and 1.6.2 as written about how to provide evidence? Therefore, we believe more examples of evidence should be provided.

While we support these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and audit challenges.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response Thank you for your comments.

SDT added guidance in the guidelines section to support use of software repositories so that integrity checks are not duplicated for each installation. Other details were also added to the guidelines section to provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard. The SDT believes Part 1.6 and the associated measure provide responsible

entities the ability to implement the verification process in a manner that is consistent with the guidelines section and avoids duplicating efforts as written. Part 1.6 applies to baseline changes after the effective date of the standard. The reliability objective is “intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates of patches to a BES Cyber System” (P. 49). Performing software verifications as part of establishing the baseline (e.g., for a new BES Cyber System) is not in scope for Part 1.6.	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA supports the revisions to CIP-010-2. However, in the GTB the SDT should clarify the meaning of this sentence: “For example, in the System and Information Integrity (SI) control family, control SI-7 suggests that the integrity of information systems and obtaining software directly from the developer.” This sentence seems to be incomplete and further words are needed to complete it.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the guidelines section to address this issue.	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	

Comment	
R1.6 brings to mind several challenges. The intent appears to be to ensure that software is validated, which is not the issue. The issue is the auditability of the requirement and its existing language. The wording "when the method to do so is available" puts additional obligations on the Responsible Entity to prove whether the methods were available or not, when the methods were available, if it was appropriate to utilize the available methods in a given circumstance. It adds additional nuance when the methods are often obtained from third parties. If it is a legacy contract and has not been updated and the method is available to other entities but not to the Responsible Entity due to the legacy contract, is the method considered available? The intent of this requirement is good but the auditability of the language is challenging at best and should be adjusted to consider how entities will be able to document and comply with the requirement language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. SDT believes the phrase 'when a method to do so is available' provides responsible entities with necessary flexibility to perform configuration management obligations. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity's software update and patch management processes. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2 that will improve the clarity of the standard.	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
• Please provide clarification to what, "verification of identity of the software source and integrity of the software" means. Please provide more examples within the Measures to ensure entities are prepared for compliance oversight expectations.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2. Additionally, the Measure was revised to include evidence of meeting the requirement using automated update mechanisms.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
SPP recommends that the drafting team provide examples to provide clarity on control design to meet the intent of the standard.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

NRG recommends that the drafting team provide examples to provide clarity on control design to meet the intent of the standard.

The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e. the cases of multiple installations of a given piece of software across many similar applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. NRG requests guidance on using trusted internal repositories as a software source so that Entity can verify once and use many

The VSL as currently written may not cover the failure to implement the process. The VSL may not include all of the combinations.

NRG has concerns with Parts: 1.6.1 and 1.6.2 as written --- For example, how would a Registered Entity be expected to provide evidence? NRG request additional examples of evidence in the Measures section of the requirement.

NRG suggests rephrasing “when the method to do so is available to the Responsible Entity from the software source” to “when the vendor supplied method to do so is available to Responsible Entity”. Otherwise the “method to do so” may be ambiguous and leaving the following questions:

How does one prove that a method is not available?

What is the line between available/unavailable? How far do you have to go?

NRG is concerned with double jeopardy potential with CIP-007 R2. NRG is concerned that it may be difficult or impossible to validate the source or verify authenticity of the patch itself which may cause the industry to not consider that patch to be available.

Likes 0	
Dislikes 0	
Response Thank you for your comments. The SDT added details to the guidelines section that provide technical considerations and examples for meeting Part 1.6.1 and 1.6.2. This includes guidance to support use of software repositories so that integrity checks are not duplicated for each installation. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. Part 1.6 provides responsible entities with flexibility to meet the reliability objective. A responsible entity could use a verification method that is provided by the vendor, or another method that is available. Techniques described in the guidelines and technical basis section are not limited to those provided by the software's vendor. An entity could demonstrate that a method to perform verification is not available by providing documentation from the software source, evidence such as a screen shot that shows the methods described in the guidance section are not available, or an attestation. The SDT believes the phrase 'when a method to do so is available' provides responsible entities with the flexibility necessary to prevent disruption of their software update and patch management processes. Thus, Part 1.6 does not impact an entity's ability and obligation to meet CIP-007 R2.	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	

ITC Holdings believes the wording of CIP-010-3 leaves a lot of room for interpretation and needs to be more prescriptive. The measures should define technical examples (e.g., denote MD5 fingerprint or hashing as being an acceptable method). Additionally, ITC recommends including Remedy in the Technical Guidance document if you can't use the file integrity method.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes Part 1.6 addresses the reliability objective for software verification contained in the project SAR and provides responsible entities with the flexibility necessary to meet the obligation. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility may be needed to prevent disruption of an entity's software update and patch management processes. SDT has added guidance in the technical guidelines section to support responsible entities in adding this objective to their configuration change management processes.	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE notes that the proposed standard is not responsive to the FERC directive. FERC Order No. 829 P. 59 specifically states "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." The Note in Part 1.6, however, states: "Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual *terms and conditions of a procurement contract*; and (2) vendor performance and adherence to a contract." Texas RE agrees that it is unreasonable to hold a registered entity accountable for a vendor's adherence to (or lack of adherence to) a contract. Texas RE agrees as the SDT claims obtaining specific controls in the negotiated contract may not be feasible at all times but Texas RE believes this is *best practice*. In fact, in most cases contracts for these types of systems typically include security provisions and set similar expectations as described in the	

standard. The proposed standards would prohibit the compliance monitor from verifying the registered entity implemented part 1.6. Moreover, this verification is to ensure that the registered entities' plans are consistent with the contract's expectations and obligations of the parties. Admittedly, there will be circumstances in which a contracts may not be consistent or silent as it pertains to the responsible entity's security management plans (e.g. existing contacts or contracts in which the responsible entity was unable to negotiate the appropriate terms into the contract.) In those circumstances, other evidence should be provided demonstrating that the responsible entity has processes to ensure the vendor is expected/obligated to act consistent with the responsible entity's cyber security risk management plans as it relates to the vendor's products or services. Therefore, the contracts should remain in scope as to demonstrate the mapping of expectations from the plan to the contract as far as vendor interactions for those specific items included in the standard and to advance best practices leading to a more reliable BES. Texas RE also recommends the SDT remove or provide clarity on the verbiage that reads, "*and when the method to do so is available to the Responsible Entity from the software source*". A potential scenario exists now where vendors will attest that identity and integrity methods are not available therefore Part 1.6 is not applicable. Texas RE notes that the words "integrity" and "authenticity" are used in the Guidelines and Technical Basis however Part 1.6 uses the words "identity" and "integrity". Are these intended to be the same?

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Part 1.6 applies to baseline changes after the effective date of the standard, regardless of whether the responsible entity has a contract with a vendor. The SDT believes the measures describe the acceptable evidence that should be used to assess responsible entity adherence to the software verification requirements.

SDT believes the phrase 'when a method to do so is available' provides responsible entities with necessary flexibility to perform configuration management obligations. Responsible entities have varying baselines, software vintages, and vendor support. Flexibility

may be needed to prevent disruption of an entity's software update and patch management processes, including obligations under CIP-007. The SDT revised the guidelines section to remove terms that are not consistent with Part 1.6
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power

Answer	
Document Name	

Comment
MEAG supports the answers and comments of Salt River Project.

Likes 0	
Dislikes 0	

Response

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

Richard Vine - California ISO - 2	
Answer	No
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments of the IRC.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx
Comment	
Malware inserted into the U.S. electric grid in year 2014 and into the electric grid and other assets in the Ukraine in December 2015 and December 2016 target nominally "low impact" assets producing high impact consequences. See integrated comments that address in part the need to upgrade protections for so-called "low impact" facilities. (Comment at end of document)	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for “industrial control system hardware, software, and services associated with bulk electric system operations”(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that	

reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	No
Document Name	
Comment	
While the IRC members do not have Low Impact Bes Cyber Systems we have multiple interfaces with our Market Participants that do have Low Impact BES Cyber Systems. This, in turn represents, risk to our BES Cyber Systems. As such we recommend that CIP-013-1 apply to Low Impact BES Cyber Systems to reduce the supply chain risk not only to the Low Impact BES Cyber Systems but to the IRC member organization's BES Cyber Systems. Note: **PJM does not support this comment**.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations"(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities	

retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.

IESO	
Answer	
Document Name	

Comment
As the IESO does not have any low impact BES Cyber Systems we abstain from answering Yes or No to this question. However, we suggest the rationale for not including Low Impact Bes Cyber Systems is not clear. We also suggest that small to medium sized Responsible Entities have the most to gain from CIP-013 as they have the fewest resources to mitigate risks from the supply chain. While the IIESO does not have Low Impact Bes Cyber Systems we have multiple interfaces with our Market Participants that do have Low Impact BES Cyber Systems. This, in turn represents, risk to our BES Cyber Systems. As such we recommend that CIP-013-1 apply to Low Impact BES Cyber Systems to reduce the supply chain risk not only to the Low Impact BES Cyber Systems but to the IRC member organization’s BES Cyber Systems.

Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations"(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	No
Document Name	
Comment	

While the initial direction of CIP-013-1 is good and provides protection for High BCS and Medium BCS, similar Cyber Assets associated with Low impact BES Cyber Systems may represent vectors for attack to High BCS or Medium BCS if left unprotected. WECC understands the reluctance of industry to incorporate Low impact BCS and their component BCA and other Cyber Assets under the CIP-013-1 purview and supports remanding SCRM issues associated with Low impact BCS to the CIP-003 Standard Drafting Team for integration into R1.2 and R2 of that Standard to ensure SCRM is integrated into those BCS at a level commensurate with the risk posed to the reliability of the BES.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The SDT does not believe development of requirements for low impact BES Cyber Systems, under either the supply chain or the CIP Modifications project, provides necessary reliability benefit commensurate with costs.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Teresa Cantwell - Lower Colorado River Authority - 1	

Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Oxy agrees with the removal of low impact BCS from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. Oxy believes that for entities that have a mixture of high, medium and low impact assets, the low impact assets would inherently benefit from the requirements applicable to high and medium impact assets as a matter of normal business practice, as the high water mark will be applied when purchasing equipment and services. This will account for a large portion of low impact BES Cyber Systems. Oxy believes it is appropriate to address the supply chain requirements using this risk-based approach. Low impact BES Cyber Systems are categorized as low impact because they inherently pose a low risk to negatively impact the Bulk Electric System. Resources should focus on those systems that have the potential for significant adverse impact on the BES. Additionally, vendors will not differentiate their product as low, medium or high impact, so as vendors address the requirements of high and medium impact entities, low impact entities will acquire the same products and services as medium and high impact entities. If low impact BES Cyber Systems were included in CIP-013-1, the costs associated with compliance would far outweigh the risk posed to the BES, in both manpower and additional equipment and services.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA appreciates the SDT's efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
None	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes. Industry supply chain management advances that would impact low impact BES Cyber Systems would be addressed by vendors through the requirements for high and medium impact BES Cyber Systems.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Duke Energy agrees with the removal of low-impact BES Cyber Systems from the applicability of CIP-013-1. Low-impact BES Cyber Systems have been subject to a risk assessment and classified low-impact since they pose a minimal threat to the BES. Also, a Responsible Entity is not required to have an inventory list of its low-impact BES Cyber Systems. If this standard were to apply to low-impact BES Cyber Systems, this would likely create a situation wherein an inventory list is necessary. This would be a significant effort, which would not likely bolster the reliability of the grid, based on the limited impact lows present to the system.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE appreciates the SDT's efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	

Comment	
Luminant believes it is appropriate to address the supply chain requirements using a risk-based approach. Low impact Cyber Systems are categorized as low impact because they inherently have a low ability to negatively impact the Bulk Electric System. We should focus our resources on those systems that have the potential for significant adverse impact on the BES. In addition, there are many types of low impact Cyber Systems. If a decision was made to put them back into the standard, there would need to be extensive work on evaluating each of these types of systems in order to determine whether there is adequate benefit to reliability to offset the cost and burden of imposing supply chain requirements for these systems.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes

Document Name	
Comment	
IPC agrees that the applicability to Lows should be removed.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	
GSOC supports NRECA's Comments of: NRECA appreciates the SDT’s efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

USI agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agree that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829.	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response. Thank you for your comments.	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
NPPD supports the position of the MRO NSRF.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA appreciates the SDT's efforts to develop the supply chain requirements under a risk-based lens.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
No Comments	
Likes 0	
Dislikes 0	
Response	

Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the removal of low impact BCS from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. SRP believes that for entities that have a mixture of high, medium and low assets, the low assets would inherently benefit from the additional requirements of medium and low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have low assets only, there would not be additional requirements based on CIP-002 risk based approach. SRP believes that including lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with lows.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
No comments	
Likes 0	

Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See Attached Comments.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	Yes
Document Name	
Comment	
BC Hydro believes that focussing on Medium and High Impact BCS instead of Low Impact is a good place to start. If insufficient risk mitigation is found to be provided here, it can always be expanded later. However, BC Hydro does not believe CIP-013-1 itself is necessary given what entities will already be doing under the other CIP v5 standards	
Likes 0	
Dislikes 0	

Response. Thank you for your comments.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE agrees with removing low-impact BCS from CIP-013-1 and agrees the current standard, as written, appropriately addresses the Commission's concerns as specified in Order No. 829. AE believes, for entities with a mixture of High, Medium and Low Impact BCS, the Low Impact B CA would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many contracts and master agreements are developed for all products and services purchased from a vendor. For entities with Low Impact BCS only, there would not be additional requirements based on the CIP-002 risk-based approach. AE believes including Low Impact BCS will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these devices. Also, controls inherent to CIP-013 and previous CIP Standards reduce the risk associated with Low Impact BCS.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

SMUD agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. SMUD believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach.

SMUD believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with Lows.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Tyson Archie - Platte River Power Authority - 5

Answer	Yes
Document Name	

Comment

PRPA agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. PRPA believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and Low requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach.

PRPA believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items. Also, controls inherent to CIP-013 and previous CIP Standards that reduce the risk associated with Lows.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Santee Cooper agrees with the removal of low-impact BES Cyber Systems from CIP-013-1. Including low-impact BES Cyber Systems will require substantial resources by a Responsible Entity it identify and maintain an inventory list of items.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	
Answer	Yes
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes

Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	

Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	

Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Lauren Price - American Transmission Company, LLC – 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE's opinion is that low impact BES Cyber Systems should be included in CIP-013-1 because industrial control systems monitor and operate BES Cyber Assets located at transmission substations, wind farms, and generation facilities. Texas RE noticed that Question 4 uses the words "hardware, computing and networking services", which are not found in CIP-013-1. Should they be used in CIP-013-1 instead of "equipment, products, and services"?	
Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations"(P. 43). High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities. The SDT used wording in CIP-013-1 that is consistent with other CIP standards. The SDT did not use the wording from Order No. 829 because it could be potentially unclear to responsible entities.
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance

Answer	
Document Name	
Comment	

No comment	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	
Document Name	
Comment	
PJM chooses to abstain from this question as we have no low impact assets.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.	
Gregory Campoli - New York Independent System Operator - 2	
Answer	No
Document Name	
Comment	
Request a 24 month implementation due to budget cycles and technical controls for other CIP Standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	No
Document Name	
Comment	
Disagree with the Implementation Plan. Standard should have language stating whether or not software installed prior to enforcement must have identify/verification completed.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. CIP-010-3 R1 Part 1.6 applies to changes to baseline. Software verification of existing baseline is not in scope.	
Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	
Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards.	

The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	No
Document Name	
Comment	
Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comment.	

The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
Performance requirements are too vague to be auditable. See related comments. (Comment at end of document)	
Likes 0	
Dislikes 0	
Response	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	No
Document Name	
Comment	

SMUD generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. SMUD feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers. SMUD is indicating a "no" response as the implementation plan does not include a pilot. The implementation of TCA CIP 010 R4 was difficult as entities did not have a model implementation to learn practical applications of the standard in operations. Other standards that had a pilot allowed entities to learn practical implementation decisions that would save money and time. Please note, SMUD is willing to participate as a pilot participant.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk. The purpose of the Implementation Plan is to propose the effective dates of the Reliability Standards. A pilot program could support entity implementation and would not impact the proposed effective dates. SDT has shared the recommendation for a pilot with NERC and ERO staff for consideration as plans are developed to support industry implementation.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

It is uncertain when purchasing activities become subject to CIP-013-1. The proposed Implementation Plan states: "Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1."

Reclamation recommends that the "General Considerations" guidance contained in the Implementation Plan pertaining to purchasing activities be included in the proposed standard.

If the "General Considerations" guidance on purchasing activities becomes part of the proposed standard, Reclamation further recommends:

- A contract becomes within scope when the entity commences its formal contract process such as when a request for proposal or solicitation is issued.
- Any direct purchase and/or any repurposed equipment is within scope prior to connecting to the Bulk Electric System as a cyber asset.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT has revised the Implementation Plan to clarify when an entity's procurement actions become subject to CIP-013-1. The general consideration section now reads:

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.

Nicholas Lauriat - Network and Security Technologies - 1

Answer	No
Document Name	

Comment	
CIP-013 R2 and/or the Implementation Plan should contain “trigger” language for R2 that clarifies an entity must implement its R1 risk management plan(s) for new procurement contracts signed on or after the Effective Date of CIP-013. Entities with no new procurement contracts or no new in-progress procurements on the Effective Date should not be expected to be able to demonstrate compliance with R2 at that time.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. SDT has revised the Implementation Plan to clarify when an entity must implement its plans. The general consideration section now reads:

> *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity’s plan) that begin on or after the effective date of CIP-013-1.*

The SDT agrees that entities should not be expected to demonstrate compliance with Requirement R2 if the entity has not initiated procurement processes when the requirement is effective.

David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request a 24-month implementation due to budget cycles and technical controls for other CIP Standards	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Request a 24 months implementation due to budget cycles and technical controls for other CIP Standards	

Recommend changing this General Consideration from Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1. To Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	

FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
GRE and the NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	

Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes. Moving the implementation date from 12 to 18 months is consistent with the CIP v5 implementation timeline for implementations. Would low impact BES Cyber Assets that might be in scope in the future have similar implementation timeline or longer?	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not considering requirements or implementation periods for low impact BES Cyber Systems.	
Mark Riley - Associated Electric Cooperative, Inc. - 1, Group Name AECI & Member G&Ts	
Answer	Yes
Document Name	
Comment	
AECI supports NRECA's comments provided below: NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the “Planned or Unplanned Changes Resulting in a Higher Categorization” section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the “Applicable Facilities” section or other language that clearly indicates these standards/requirements do not apply to “low” entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	Yes
Document Name	
Comment	
GTC supports NRECA comments: NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	

Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	

Southern recommends that the SDT consider addressing previous issues with the Implementation Plan versions between CIP V5, V6, V7, etc., where Implementation Plans were “chained” together and there was not an Implementation Plan that contained all the necessary requirements in a single source. Southern strongly recommends producing a consolidated Implementation Plan.

Southern recommends that NERC and the SDT(s) consider addressing issues with the Implementation Plan versions between CIP V5, V6, V7, and Supply Chain, as Implementation Plans are “chained” together and there is no one Implementation Plan that contains all the necessary requirements in a single source. Implementation Plans for the CIP standards cover several important areas:

Implementation schedules of new or modified CIP standard requirements.

Implementation schedules for newly identified cyber assets brought into scope with current requirements based on planned or unplanned changes in the BES assets, or those from newly registered NERC entities. (previously known as IPFNICANRE – Implementation Plan for Newly Identified Cyber Assets or Newly Registered Entities)

Implementation schedules for BES Cyber Systems already in scope that change impact levels due to planned or unplanned changes in the BES.

As an example, the last page of the Implementation Plan for CIP-003-7 states that CIP-003-6 is retired upon approval of CIP-003-7, yet it chains to the CIP-003-6 Implementation Plan to tell entities how to handle cyber systems that change impact categorization. The CIP-003-6 implementation plan simply says it replaces *parts* of the V5 implementation plan for the modified standards in that revision. Only the V5 plan addresses the 2nd bullet point above. Responsible Entities are left to unravel three different plans with supply chain adding yet another to get one picture of what is due when and knowing how to handle BES changes that affect cyber system identification and impact categorization.

As we go forward, we need a better solution. Parts of an implementation plan, such as bullets 2 and 3 above, need to live on indefinitely. Other parts, such as the schedule of new or modified requirements, need to live until those dates have passed. Chaining all

of this together through numerous documents as the CIP standards continue to evolve and grow to cover new areas is not a sustainable solution that promotes clarity in knowing the compliance obligation in a changing environment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that Implementation Plans should avoid or, at a minimum provide clear details of, any overlap with pending effective dates of pending Reliability Standards requirements so that entities have clarity on the impact of implementation on their compliance obligations. The proposed Project 2016-03 Implementation Plan is not tied to requirements that have future effective dates, thereby avoiding some of the expressed concerns. Furthermore, the Implementation Plan has been revised to include provisions for unplanned changes so that it is not reliant on these provisions from Implementation Plans associated with other standards.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
Disagree with the Implementation Plan. Standard should have language stating whether or not software installed prior to enforcement must have identify/verification completed.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. CIP-010-3 R1 Part 1.6 applies to changes to baseline. Software verification of existing baseline is not in scope.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	

Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	

Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
As mentioned above, WECC supports the CIP-013-1 implementation plan, including the expectation for the initial performance of the R3 review and approval on or before the effective date.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	Yes
Document Name	
Comment	
CHPD supports these changes.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes

Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
We agree with APPA's submitted comments, including: Suggesting a change in wording to say that the Supply Chain Risk Management Plan must be used on or after the implementation date rather than saying that contracts on or after that date are within scope of CIP-013. Clarification should be made about if/when existing contracts or agreements come into scope.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows: *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of*	

cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
PRPA generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. PRPA feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE generally agrees with an 18-month implementation plan but, would prefer 24-months. AE feels a 24-month timeframe is more appropriate and gives entities additional time to align budgets and develop processes with vendors and suppliers. As a municipal utility, AE's procurement process is quite long.	

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk. The SDT also believes the flexibility provided in the requirements supports the various procurement processes that may be used by responsible entities.

Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx

Comment

See attached comments

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions for unplanned changes consistent with other CIP standards.

The SDT has revised the General Considerations section in the Implementation Plan as follows:

> *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.*

Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	

Recommend changing this General Consideration from

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date of the CIP-013-1. Make corresponding change to the CIP-013 R2 note.

And

CIP-005-6 and CIP-010-3 must be implemented 18 months after the implementation date of the CIP-013-1

Implementation Plan does not handle unplanned changes such as IROLs or registration, etc.

Request a 24 month implementation of CIP-013-1 due to budget cycles and technical controls for other CIP Standards

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT revised the General Consideration section to incorporate the suggested wording, and included provisions in the Implementation Plan for unplanned changes consistent with other CIP standards.

The SDT does not believe it is necessary to delay implementing CIP-005-6 and CIP-010-3 until after CIP-013-1. Procurement actions taken according to the entity's Supply Chain Cyber Security Risk Management Plan can support the new requirements in CIP-005-6 and CIP-010-3, however the new CIP-005-6 and CIP-010-3 requirements are written so that they are not dependent on these procurement actions.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. SRP feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While in overall agreement with the updated Implementation Plan, ACEC does have the following concern:	

The second paragraph in the section "General Considerations" states "Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1." Based upon the above wording it could be understood that Master Supply Agreements (MSAs) would need to be changed in the first RFP after implementation of the new standard. The paragraph should state specifically that this is not required, and that the plan can allow MSAs to exist as is until it is time to review in the normal procurement process.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows: *In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.*	
Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	Yes
Document Name	
Comment	
NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan. Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.	

Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Thank you for your statement under Initial Performance of Periodic Requirements, that the supply chain security risk management plans need to be approved on or before the effective date of CIP-013-1.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	
Comment	
Comments: NPPD supports the position of the MRO NSRF. NPPD believes a 24-month implementation should be used due to budgeting and tthe technical implementation requirements for the other CIP Standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	
Recommend changing this General Consideration from:	

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To:

Supply Chain Risk Management plan must be used by appropriate procurement processes that begin on or after the implementation date. Make corresponding change to the CIP-013 R2 note.

Further, USI requests clarification on if/when existing contracts, master contracts, or long-term maintenance agreements that re-opened for renegotiation or put in use, come into the scope of CIP-013.

The implementation Plan does not handle unplanned changes such as IROLs or registration, etc. Request that the Implementation Plan be modified to handle entities that meet the applicability after the effective date of the standard.

USI believes a 24-month implementation should be used due to budget cycles and technical controls for other CIP Standards.

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows:

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.

The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards.

The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.

Guy Andrews - Georgia System Operations Corporation - 4	
Answer	Yes
Document Name	
Comment	

GSOC supports NRECA's Comments of:

NRECA supports the new implementation plan timeframe. However, this implementation plan unintentionally removes the provisions for additional time to implement unplanned changes in CIP-005 and CIP-010 that was provided in the V5 and V6 implementation plans. NRECA strongly requests that the language from the "Planned or Unplanned Changes Resulting in a Higher Categorization" section of the CIP V5 standards implementation plan be re-inserted into the supply chain implementation plan.

Additionally, the absence of the "Applicable Facilities" section or other language that clearly indicates these standards/requirements do not apply to "low" entities is missing in the Implementation Plan. NRECA urges the SDT to add this section the Implementation Plan.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards, and to clearly indicate the standards to not apply to entities that do not have any medium or high impact BES Cyber Systems.

Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

NRG recommends changing this General Consideration from:

Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

To

Supply Chain Risk Management plan must be used by the procurement processes that begin on or after the implementation date. Please consider making the corresponding change to the CIP-013 R2 note

The Implementation Plan does not appear to address unplanned changes such as IROLs or registration, etc.

NRG requests consideration of a 24 month implementation due to budget cycles and technical controls for other CIP Standards

Likes 0	
Dislikes 0	

Response, Thank you for your comment. The SDT has revised the General Considerations section in the Implementation Plan as follows:

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1.

The SDT has revised the implementation plan to include provisions for unplanned changes consistent with other CIP standards.

The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Daniel Grinkevich - Con Ed - Consolidated Edison Co. of New York - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Laura Nelson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE requests that the SDT provide its rationale for extending the effective date from 12 to 18 months. For example, it is unclear whether the SDT believes more certainty is required regarding the necessary technical deployments for compliance with the Standard as some commenters suggested to justify the extended implementation period.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees with commenters that the proposed requirements can be impacted by budget cycles, which can extend beyond 12-months. The SDT believes the proposed requirements can be implemented within the 18-month implementation period, and that this period appropriately reflects the urgency needed to address the reliability risk.	
Richard Vine - California ISO - 2	
Answer	
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	

Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2

Answer	No
Document Name	

Comment
ERCOT joins the comments of the IRC.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy

Answer	No
Document Name	

Comment
Duke Energy suggests the drafting team consider implementing a staggered approach to the VSL(s) specifically to CIP-013-1 R2. As written, an entity could implement all aspects but one sub-part of the risk management plan, and the violation would have a VSL of Severe. We recommend the drafting team consider a more equitable approach and stagger the VSL(s) similar to the approach used in R1 of CIP-003-6.

Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No
Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
We do not agree with the VRF Justification for CIP-013-1 R1, FERC VRF G5 with the new redline. Agree with the words that were redline out.	

CIP-010 – VSL does not cover the failure to implement the process and therefore does not include all of the combinations. Consequently, we request that there be lower severity levels when a single aspect of the requirements is missing. Request that that the term “elements” be included in CIP-013 R1.2 (as shown in comments for question 1) to clearly align with the VSLs for this requirement.	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	
Response. Thank you for your comment. The SDT agrees with the suggested change to the VRF justification for CIP-013-1 Requirement R1. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2. For all CIP-010 Requirement R1 parts, implementation of the specified processes is covered under existing Lower, Moderate, High, and Severe VSLs as a collective configuration change management process. The SDT believes it has integrated new Part 1.6 in a manner that is consistent with the other parts in approved CIP-010-2 Requirement R1. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly.	
Richard Kinas - Orlando Utilities Commission - 5	
Answer	No
Document Name	
Comment	
The VSL for R2 only provides for a Severe VLS. It is unclear what is meant by "did not implement". If your plan has 5 areas within it and 4 of the 5 were fully implemented, has the plan been implemented? I contend yes however not fully implemented. The VSL were created to identify how far of the complaince mark an entitiy fell. This VLS completly fails to perform this action. While at the same time the VSL for R3 utilizes arbitrary calendar months for clear VLS seperation between lower and severe. Both of these VLS provide little benefit to industry in assessing the real impact to the BES based on an entity missing the complaince mark.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	

Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
We support APPA's comments that the original wording is better than the new redline of the VRF justification.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees with the suggested change to the VRF justification for CIP-013-1 Requirement R1.	
Thomas Foltz - AEP - 5	
Answer	No
Document Name	
Comment	
While an important topic, at this time AEP does not agree that risks associated with violations of these draft standards is a “Medium” risk to the BES. AEP recommends the Violation Risk Factor for each of the requirements CIP-013-1 R 1-3 be considered “Lower.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT developed the VRFs to conform to NERC and FERC guidelines as explained in the VRF/VSL Justification.	

Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es) for its newly procured BES Cyber Systems that address the following elements, as applicable:”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
: For CIP-013-1, R3, Dominion recommends the following alternate VSL values. • Low – No change • Moderate – 16-18 calendar days • High – greater than 18 calendar days	

• Severe – When a review has never been performed	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT established the levels to be consistent with approved CIP standards and does not see benefit to adopting alternate levels.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD asks that that the term "elements" be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. "***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:"*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term 'elements' from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD asks that that the term “elements” be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement. “***1.2.*** *One or more process(es)* ***for its newly procured*** *BES Cyber Systems that address the following* ***elements****, as applicable:”*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	No
Document Name	

Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	

Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
The IRC suggests the drafting team add more thresholds to the VSLs for R2 of CIP-013-1 and that it be aligned more closely with that of R1, rather than making it binary. The cyber security risk management plan will be fairly large and missing small portions of the plan should not immediately result in a Severe VSL.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	
IESO	
Answer	Yes
Document Name	
Comment	

None	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
None	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
No comments.	
Likes 0	

Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
There should be lower, moderate and high VSLs for R2, (not implementing portions of the requirement). PJM suggests using the language in the lower, moderate and high R1 VSLs as a starting point.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT has revised the VSL for CIP-013-1 Requirement R2 to specify four levels of possible non-compliance.	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	Yes
Document Name	
Comment	
Yes for CIP-005-6 and CIP-010-3 only	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	

Answer	Yes
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	

No Comments	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	
Comment	
YES for CIP-005-6 and CIP-010-3 only	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP agrees with the VRFs and VSLs for CIP-010 and CIP-013. SRP believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to	

determine and did not have a method to disable. SRP would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. SRP requests that the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE agrees with the VRFs and VSLs for CIP-010 and CIP-013. AE believes the VRFs and VSLs for CIP-005 should be updated to reflect the same approach taken in CIP-010. The VSL for CIP-005 results in a severe penalty if an entity does not have a method to determine and does not have a method to disable. AE would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. AE requests the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	

Response Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term 'elements' from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
SMUD agrees with the VRFs and VSLs for CIP-010 and CIP-013. SMUD believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to determine and did not have a method to disable. SMUD would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. SMUD requests that the term "elements" be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term 'elements' from the VSL for CIP-013-1 Requirement R1 Part 1.2.	

Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	
PRPA agrees with the VRFs and VSLs for CIP-010 and CIP-013. PRPA believes that the VRFs and VSLs for CIP-005 should be updated to reflect the same approach that was taken in CIP-010. The VSL for CIP-005 results in a severe penalty if the entity did not have a method to determine and did not have a method to disable. PRPA would prefer a High VSL penalty if the entity has a process to determine but does not have a process to disable and vice-versa if the entity did not have a process to determine but does have a process to disable. PRPA requests that the term “elements” be included in CIP-013 R1.2 (as shown above) to clearly align with the VSLs for this requirement.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The SDT agrees that another level can be specified for CIP-005-6 and has revised the VSL accordingly. The SDT has removed the term ‘elements’ from the VSL for CIP-013-1 Requirement R1 Part 1.2.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	

No Comment.	
Likes 0	
Dislikes 0	
Response	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
WECC has no issues with the VSLs or VRFs from a CIP Auditor perspective.	
Likes 0	

Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
William Harris - Foundation for Resilient Societies - 8	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wendy Center - U.S. Bureau of Reclamation - 5	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	

Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	No
Document Name	
Comment	
The requirements aren't vetted enough to make a fair judgement.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Timothy Reyher - Eversource Energy - 5	
Answer	No
Document Name	
Comment	
Implementation Guidance for R3	

Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:” Implementation Guidance for R3 – Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. NERC Compliance Guidance Policy provides a means for any NERC registered entity to document examples of approaches and vet them through an approved organization for endorsement consideration by the ERO Enterprise.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	No
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	No
Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No

Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	

CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	
The existing guidance still provides no scope of cyber security risks that should be considered, and without context, many of the proposed actions have no guidelines or measurements for "success" or "failure" or acceptability; nor are there suggested acceptable mitigations if a criterion is not completely met, since there is no clear objective. Furthermore, there is no allowance made for a continuous process, where, as a result of products already being used in BES Cyber Systems and subjected to the existing CIP standards, cyber security risks	

associated with networks, products and vendors are evaluated on an on-going basis. Detailed changes and additions are outlined in a separate redline Draft Implementation Guidance document that has been forwarded to NERC and the SDT. A summary of the proposals is as follows:

1. Throughout the document, the term 'controls' should be changed to a term that more closely reflects the language in the proposed standard. Dominion recommends using 'terms and conditions'.
2. On page 2, dominion recommends clarifying that cyber security risks are limited to supply chain with the addition of 'supply chain' prior to each use of the term cyber security risks.
3. In addition to the clarifying language in item #2 above, Dominion recommends adding the following to more clearly define the term 'supply chain cyber security risk:

(1) procuring and installing un-secure equipment or (2) procuring and installing un-secure software, including purchasing counterfeit software, or software that has been modified by an un-authorized party, (3) unintentionally failing to anticipate security issues that may arise due to network architecture, (4) unintentionally failing to anticipate security issues that may arise during technology and vendor transitions for BES Cyber Systems). The additional bullets could be sub-bullets under the appropriate of these four broad areas as examples rather than individual, isolated items.

4. Dominion recommends deleting the third paragraph on page 2. This paragraph appears to be creating new/different obligations. The language appears to create confusion and calls out Section 1.2.5 specifically for no apparent reason.

5. The language in blue boxes throughout the document should be retained and included in the text of the document.

6. It is unclear what the purpose of including certain language in a blue box is.

7. Section headings should be included with each of the examples. Also, the bulleted format makes it unclear if one, all, or a certain number of bulleted items need to be performed to achieve compliance.

8. Add the following example under R1.1:

Develop an approved vendor/products list. When planning a BCS, the RE should evaluate the following items:

-
  - Vendors
  - Products
  - Network Architecture
  - Network Components.

The RE should document (which may be limited to the baseline and cyber vulnerability assessment (CVA) required for a new product) any risks (i.e. 1) procuring and installing un-secure equipment or (2) procuring and installing un-secure software, including purchasing counterfeit software, or software that has been modified by an un-authorized party, (3) unintentionally failing to anticipate security issues that may arise due to network architecture, (4) unintentionally failing to anticipate security issues that may arise during technology and vendor transitions for BES Cyber Systems) identified and how the risks are mitigated for any "item" that deviates from those vendors, products, network architecture, and network components already being used within the RE's BCS infrastructures, which are required to comply with existing CIP standards.

9. The second bullet in Section 1.2.2 should be removed. It is already addressed under Section 1.2.1.

10. In Section 1.2.3, the end of the first bullet could state be clarified as follows:

Delete 'within a negotiated period of time of such determination' and replace with "to allow the RE to remove access within 24 hours of the determination, consistent with existing CIP standards"

Replace 'breaches' with 'vulnerabilities' for clarity and consistency'.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. Per NERC's Compliance Guidance Policy, various organizations are qualified to vet proposed Implementation Guidance prior to requesting ERO Enterprise endorsement.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No
Document Name	
Comment	
CHPD is uncertain if this new approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. CHPD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner with regard to balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, CHPD would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	

Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No
Document Name	
Comment	
The Implementation Guidance only identifies items that could be evaluated in developintg a Supply Chain Cyber Security program, but does not provide an example or guidance on how to implement the program. Without this guidance, it is impossible to understand how to comply with CIP-013-1 in a cost-effective and compliant manner.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the Implementation Guidance describes examples of how to implement the requirements.	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	No
Document Name	
Comment	
We agree with APPA's submitted comments concerning "vendor" not being a NERC-defined term and that the Implementation Guidance for R3 does not adequately explain compliance needs.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro does not agree with the examples as compliance will be challenging. It would require us to have sufficient authority over the vendor (which will not be the case in most situations). There is also no way to ensure that a vendor is being completely transparent regarding cyber vulnerabilities in their product. Such disclosure could have other impacts on their business with other clients. This would be a dis-incentive for disclosure. BC Hydro does not believes CIP-013 is necessary and cyber control is already achieved with the rest of the CIP v5 standard requirements around change control, testing and ongoing systems monitoring.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the examples provided in the ERO-Enterprise endorsed Compliance Guidance can be implemented by responsible entities using their procurement processes. The requirements in CIP-013-1 do not require responsible entities to impose obligations on vendors. The requirements address the reliability objectives contained in the project Standards Authorization Request.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	No
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.

The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. NERC Compliance Guidance Policy provides a means for any NERC registered entity to document examples of approaches and vet them through an approved organization for endorsement consideration by the ERO Enterprise.

Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	

It is uncertain when purchasing activities become subject to CIP-013-1. The proposed Implementation Plan states: “Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.”

Reclamation recommends that the “General Considerations” guidance contained in the Implementation Plan pertaining to purchasing activities be included in the proposed standard.

If the "General Considerations" guidance on purchasing activities becomes part of the proposed standard, Reclamation further recommends: • A contract becomes within scope when the entity commences its formal contract process such as when a request for proposal or solicitation is issued. • Any direct purchase and/or any repurposed equipment is within scope prior to connecting to the Bulk Electric System as a cyber asset.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. Response is provided in preceding section.	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	No
Document Name	
Comment	
There is inconsistency between the Implementation Guidance and CIP-010, R1. The requirement states "For 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". The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The requirement wording suggests it applies for any change but the Guidance suggests that for some changes, such as patches, it would not apply. Oncor believes that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore, it is believed that the best solution is to modify the Guidance.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT has not developed Implementation Guidance for CIP-010-3. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	No
Document Name	
Comment	
Definition of vendor is not a NERC defined term. The term “vendor” is also used in the proposed CIP-005. USI believes the SDT should provide guidance regarding the use of the term “vendor.” If “Vendor” is not defined by NERC, the Guidance should recommend that Entities include their definition of “vendor” in their plan(s). **Implementation Guidance for R3** Neither main bullet meets compliance because both only deal with the review and not the approval. Therefore, USI recommends changing: ”Below are some examples of approaches to comply with this requirement: “ to “Below is an example of an approach to comply with the review requirement required by: “ In addition, we recommend removing this language from the second main bullet, since it is beyond the Requirement: “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.” Also, there should be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comment.

The SDT believes the description of *vendor* in the Rationale section gives clarity to the CIP-013 requirements without limiting flexibility needed by responsible entities for developing and implementing cyber security risk management plans that meet the entity's procurement and cyber security needs. This description and all information in the rationale sections remain with the standards in the supplemental material section to inform Responsible Entities, compliance, and enforcement staffs.

The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address the concerns. NERC Compliance Guidance Policy provides a means for any NERC registered entity to document examples of approaches and vet them through an approved organization for endorsement consideration by the ERO Enterprise.

CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.

Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

- The language within the Implementation Guidance contradicts the language within CIP-013. (i.e. System-based approach). The Implementation Guidance is not auditable, however, the Standard and Requirements are. EDPR NA suggests that the Implementation Guidance is eliminated and further support are provided within the Measures for a Registered Entity and auditor's reference.
- There are numerous items in which vendors will not provide information on unless an entity is willing pay significant increases (risks, training, methodologies, threats, etc.)

• EDPR NA also suggests that NERC utilize a pilot program to test these requirements prior to enforcing the implementation of CIP-013 to all Registered Entities. • Please provide more support with respect to the expectations and possible evidence for Requirement 2.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. Furthermore, ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) staffs give deference to the examples in endorsed guidance when conducting compliance monitoring activities. The SDT believes an entity can use a system-based approach in its Supply Chain Cyber Security Risk Management plan(s) as described in the Implementation Guidance to comply with Requirement R1. The examples provided in the ERO-Enterprise endorsed Compliance Guidance can be implemented by responsible entities using their procurement processes. The requirements in CIP-013-1 do not require responsible entities to impose obligations on vendors. CIP-013-1 does not obligate entities to obtain specific contract provisions, preserving entity flexibility to make cost decisions. The SDT agrees that a pilot program could support entity implementation and would not impact the proposed effective dates. SDT has shared the recommendation for a pilot with NERC and ERO staff for consideration as plans are developed to support industry implementation. The examples of approaches described in the section titled 'Implementation Guidance For Requirement R1', when used in planning and procurement as specified in the entity's plan, provide an example of a compliance approach to meeting Requirement R2.	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	No

Document Name	
Comment	
MMWEC supports comments submitted by APPA.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states, in relevant part, “For 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.”

The Guidelines and Technical Basis section heading “Software and Authenticity,” paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application.

Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. SPP recommends that the SDT review the Guidelines and the draft standard for consistency and resolution. In addition, SPP recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines. SPP notes that there is no corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management. CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	
NRG has concerns that the Implementation Guidance for R3 (main bullet) may not meet compliance because both only deal with the review and not the approval. NRG recommends that the NERC SDT consider changing "Below are some examples of approaches to comply with this requirement:" to "Below is an example of an approach to comply with the review requirement required by:"	

NRG has concerns that the Implementation Guidance for R3 – (specifically): "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed." Therefore, NRG recommends that the NERC SDT consider removing this language from the second main bullet, since it is beyond the Requirement. There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1. The requirement states, in relevant part, "For 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." The Guidelines and Technical Basis section heading "Software and Authenticity," paragraph three on page 39, states: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application. Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. NRG recommends that the SDT review the Guidelines and the draft standard for consistency and resolution. In addition, NRG recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines. NRG notes that there is no corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management. CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	No
Document Name	
Comment	
ITC Holdings agrees with the below comment submitted by SPP: There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1. The requirement states, in relevant part, “For 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.” The Guidelines and Technical Basis section heading “Software and Authenticity,” paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.” The wording of the CIP-10-3 R1.6 Guidelines and Technical Basis section seems to imply that every time a patch/software is downloaded it does not have to be checked. Based on how the standard is written, the software source and the software must be verified each time	

something is downloaded. Even if that software was previously downloaded, the source must be validated and so must the software before application. Furthermore, the requirement wording suggests it applies for any change but the Guidelines suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the Guidelines are not, the Guidelines become superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. SPP recommends that the SDT review the Guidelines and the draft standard for consistency and resolution. In addition, SPP recommends that because automated patch deployment solutions should be able to verify the identity and integrity of the patch, the SDT consider allowing for this method of verification in the Measures or Guidelines. SPP notes that there is no corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-010-3 Measure and the Guidelines and Technical Basis section have been revised to address the stated concern with automated patch management. CIP-005-6 includes Rationale. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
As stated in the CIP-013 comments in question 1 above, the guidance needs to clarify what constitutes an incident (such as only actual breaches).	
Likes 0	
Dislikes 0	
Response	
Aaron Cavanaugh - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
Yes, and BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply	

only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	
Answer	Yes
Document Name	
Comment	
The understanding of the intent and purpose of CIP-013 is very dependent on the Implementation Guidance document. We are concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such we would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards	

development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement.	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
The Guidance for CIP-013-1 R3 should include the term 'approved' since an Entity wouldn't comply with the requirement with just a review.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	

Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	Yes
Document Name	
Comment	
Yes, the Compliance Guidance policy does provide industry with direction for implementation. However, those guidance details are not written in the requirements, measures or Reliability Standard Audit Worksheet (RSAW) and cannot be relied upon in preparation of an audit. ACES would suggest, at a minimum, that these guidelines be written in the Supply Chain Management RSAWs in the section 'Notes for an Auditor'. By placing this information in the RSAW, it gives industry additional reassurance that each region will audit Supply Chain Management consistently.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees and will provide this feedback to the RSAW Task Force.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	Yes
Document Name	
Comment	
Implementation Guidance for R3	

Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:” Implementation Guidance for R3 – Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns.	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
No additional comments.	
Likes 0	
Dislikes 0	
Response	

Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	

Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes

Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	

Comment	
ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Richard Vine - California ISO - 2	
Answer	Yes
Document Name	
Comment	
The ISO supports the comments of the Security Working Group (SWG)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Implementation Guidance for R3	

Neither main bullet meets compliance because both only deal with the review and not the approval. Recommend changing “Below are some examples of approaches to comply with this requirement:” to “Below is an example of an approach to comply with the review requirement required by:” Implementation Guidance for R3 – Recommend removing this language from the second main bullet, since it is beyond the Requirement “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns.	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
For consistency and clarity between sub-requirement 1.2.2. and the CIP-013-1 Implementation Guidance, we suggest that “cyber security incident(s)” be removed from the examples for 1.2.2. This verbiage should be replaced with either “vendor-identified incidents” or “security event(s)” as referenced in the examples for 1.2.1.	
Likes 0	

Dislikes 0	
Response Thank you for your comment. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The responsible entity has flexibility to use its preferred wording in its cyber security supply chain risk management plan.	
Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
The guidance relative to R1.2.2 and R1.2.6 partially address WECC's concerns as stated in Bullet 2 above. In general, the example approaches provide good guidance to industry on ERO expectations for compliance with the various Requirements and Parts. No other issues noted.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	

Dislikes 0	
Response. Thank you for your comment.	
Shawn Abrams - Santee Cooper - 1	
Answer	Yes
Document Name	
Comment	
The intent and purpose of CIP-013 is very dependent upon the Implementation Guidance document. We appreciate the hard work of the SDT to provide this document to industry and it has valuable information. Additionally, there is no guarantee this document will be approved by NERC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

PRPA generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. PRPA is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, PRPA would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard.

R3: PRPA requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed."

Request that there be corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not

duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.

Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
In the guidance for Requirement R1, Part 1.2.5, CenterPoint Energy believes including all third-party hardware, software, firmware, and services goes beyond the scope of the requirement. Most systems consist of components or services from numerous third-party companies. The vendor of such systems may not have direct contact with third-party companies. The level of third-party components or services that could be expected to be included may be quite extensive and therefore make it impractical for the vendor to commit to such issues in contract provisions.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the examples in the Implementation Guidance for Part 1.2.5 show a way for a responsible entity to seek information through its procurement processes that may be helpful in addressing a valid security concern associated with vendor software. Responsible entities may use other approaches to meeting the obligation of Part 1.2.5.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	
SMUD generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. SMUD is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, SMUD would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard. R3: SMUD requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. “Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.” SMUD also requests that there be corresponding “Guidelines and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the “Guidance and Technical Basis” sections in each Standard and the intentional flexibility of CIP-013 in particular. AE has concerns about the possibilities NERC and the Regions: (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, AE would prefer to see the new “Implementation Guidance Document” supplemented with “Guidance and Technical Basis” sections in each Standard.	

R3: AE requests the following language be removed from the second main bullet, because it is out-of-scope for this Requirement: "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed." AE requests there be corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2, Parts 2.4 and 2.5 and CIP-010-3 R1.6.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes

Document Name	
Comment	
Make sure the Compliance Guidance is in the scope of standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
As mentioned in previous comments, this document provides implementation guidance on CIP-013, but additional guidance on implementation of the CIP-010 and CIP-005 controls is requested, perhaps in the Supplemental Material sections. Particularly CIP-005 R2.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. The CIP-010-3 Guidelines and Technical Basis section has been revised to provide additional guidance. CIP-005-6 includes guidance in the Rationale section for Requirement R2. The Rationale will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
SRP generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. SRP is concerned about the possibilities that NERC and the Regions (1) may not endorse the separate implementation guidance at all, (2) may not endorse the guidance in a timely manner as regards balloting, and (3) may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, SRP would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard. R3: SRP requests that the following language be removed from the second main bullet, since it is out of scope for this Requirement. "Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed." Request that there be corresponding "Guidelines and Technical Basis" or "Rationale" for CIP-005-6 Requirement R2 Parts 2.4 and 2.5 and CIP-010-3 R1.6.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The CIP-013-1 Implementation Guidance has been endorsed by the ERO Enterprise. In developing the document, the SDT is being consistent with the board approved Compliance Guidance Policy which states that Implementation Guidance is the appropriate place to describe examples of approaches for complying with the standard. The SDT is not duplicating the material in the Guidelines and Technical Basis section because the examples pertain to compliance approaches. In the event that FERC requests revisions to CIP-013-1, the SDT agrees that the endorsed Implementation Guidance would not be effective since it applies to CIP-013-1. However, any revisions to CIP-013 required to respond to FERC directives must go through the standards	

development process, including stakeholder commenting and balloting. Industry could again develop revised guidance during the standards development process and submit it to the ERO Enterprise for endorsement. The SDT is not developing revisions the ERO Enterprise-endorsed Implementation Guidance at this time. The SDT agrees that revisions to the Implementation Guidance for Requirement R3 could be developed to address these concerns. The SDT has included Rationale for CIP-005-6 Requirement R2 Parts 2.4 and 2.5, and both Rationale and Guidelines and Technical Basis for CIP-010-3 R1.6. The Rationale section will be moved to the Supplemental Material section of the standard following NERC Board adoption.	
Andrew Meyers - Bonneville Power Administration - 6	
Answer	Yes
Document Name	
Comment	
Yes, and BPA disagrees with the language in Requirement R3 requiring the CIP Senior Manager or delegate approve the supply chain cyber security risk management plans. Other CIP standards, such as CIP-003-6, Requirement R1, require CIP Senior Manager approval of "policies," not "plans." In Order No. 829, the Federal Energy Regulatory Commission stated, "*Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1*, the Reliability Standard should require 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." Order No. 829 at P46 (emphasis added). Requiring CIP Senior Manager approval of plans is not consistent or similar to requiring approval of policies because plans are more tactical and numerous than policies. CIP Senior Manager approval should apply only to overarching strategic documents, and not to approval of highly detailed plans for implementation of processes. Instead, CIP-013 should be added to the list of policies requiring CIP Senior Manager approval in CIP-003-6, Requirement R1.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment. Requirement R3 addresses the Order No. 829 directive for requiring CIP Senior Manager review and approval of the plan. (P. 46). The SDT believes it is appropriate to allow entities to have flexibility in determining whether the CIP Senior Manager or delegate should review and approve the plan. CIP-003-6 provides for policy review by CIP Senior Manager only	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
While in overall agreement with the Implementation Guidance for CIP-013, ACEC does have the following concern: In the Implementation Guidance for R1 Section of the document, the subsections for implementation of Requirement R1 Parts 1.2.1, 1.2.2, 1.2.4 and 1.2.5 use the generic term “vendor(s)” in discussing these Software Authenticity and Integrity issues. To help in ensuring that these requirements are implemented in an effective manner, it is recommended that the SDT add a clarification item, noting that these requirements be addressed by the OEM providing the hardware and/or software, not a third-party such as an integrator.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT believes the ERO-Enterprise endorsed Implementation Guidance provides appropriate guidance as written and does not limit the responsible entity’s flexibility to address relevant security topics with the OEM. However the SDT believes it may not be practical for responsible entities to address the security topics with the OEM because the responsible entity may not have a relationship with the OEM that will allow the responsible entity to address the topics through its procurement processes.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	Yes
Document Name	

Comment	
N&ST has no disagreement with the example approaches contained in the Guidance but believes that while they may represent reasonable courses of action for large entities, they are likely to be far beyond the capabilities of small ones. N&ST believes an entity whose combined BES operations, OT support, and CIP compliance teams comprise fewer than 10 individuals would be hard-pressed to "form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es)." N&ST also believes, based on experience with CIP V1 – V5 cyber security training requirements, that large vendors with many BES customers will balk, sooner or later, at being asked to respond to a multitude of risk assessment requests, questionnaires, meetings, etc., each one different from the previous ones, and will instead incline towards providing a standardized set of information about their internal risk management programs and how they are applied to their products and services.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The examples in the Implementation Guidance describe some ways to be compliant with CIP-013-1. The SDT agrees that the examples may not be the most efficient or effective approaches for all responsible entities. The SDT believes including relevant cyber security topics in the procurement processes will provide reliability benefit even if some vendors do not provide all of the desired information or support requested terms.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.	
Chris Scanlon - Exelon - 1	
Answer	Yes
Document Name	
Comment	
Exelon thanks the SDT for submitting the draft Implementation Guidance for CIP-013. Does the SDT also intend the develop draft Implementation Guidance for the revised/added sections of CIP-005 and CIP-010? If so, is there a timeline that can be shared with Industry participants?	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT is not developing Implementation Guidance for CIP-005 and CIP-010.	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

IESO	
Answer	Yes
Document Name	
Comment Note: the following comment is the same as identified for question 3.	
None	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes
Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	

Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Don Schmit - Nebraska Public Power District - 5	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.	
William Harris - Foundation for Resilient Societies - 8	
Answer	No
Document Name	
Comment	
We consider the requirements to be burdensome, and impractical for many or most electric utilities without providing needed protection of the cyber supply chain. We would suggest at the outset adoptioon of a separate FERC rulemaking to detect, report, mitigate and remove malware from the bulk electric system.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	No
Document Name	
Comment	
By placing those comments and guidance in the Implementation Guidance does not provide industry protection during an audit in defining ‘cost effective manner’. If it is important to communicate to industry that Supply Chain Management can be managed in a ‘cost	

effective manner', then that should be detailed in the standards. 'Cost effective manner' is an undefined term and will be different for each entity, budget and their resources. The focus should be modified to a 'risk reduction manner' or 'risk appropriate manner'.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
LeRoy Patterson - Public Utility District No. 2 of Grant County, Washington - 6	
Answer	No
Document Name	
Comment	
There is not enough clarity in the proposed language to make that assessment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Document Name	
Comment	

NRG is cognizant and appreciative of the flexibility provided in proposed CIP-013-1 and the draft Implementation Guidance but at this time cannot speak to whether the implementation of these requirements will be cost effective. Additional internal analysis is needed to inform NRG's evaluation as to the cost-effectiveness of the proposal.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Shannon Mickens - Southwest Power Pool, Inc. (RTO) - 2 - SPP RE, Group Name SPP Standards Review Group	
Answer	No
Document Name	
Comment	
SPP is cognizant and appreciative of the flexibility provided in proposed CIP-013-1 and the draft Implementation Guidance but at this time cannot speak to whether the implementation of these requirements will be cost effective. Additional internal analysis is needed to inform SPP's evaluation as to the cost-effectiveness of the proposal.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Heather Morgan - EDP Renewables North America LLC - 5	
Answer	No
Document Name	
Comment	

By asking vendors to enforce these requirements, service costs will dramatically increase which will put a further strain on the electric industry.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Don Schmit - Nebraska Public Power District - 5	
Answer	No
Document Name	
Comment	
This new standard will put additional burden on entities. It is going to take considerable time to implement and negotiate new contracts. It is also up to the entity to provide adequate documentation to prove compliance but it will still be based on the auditor discretion if an entity has done enough. As with similar requirements in the nuclear industry we believe that contract pricing will increase due to the Standard requirements placed on the vendors via industry and may result in reduction of vendor options.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Nicholas Lauriat - Network and Security Technologies - 1	
Answer	No
Document Name	
Comment	

N&ST believes the approaches to meeting CIP-013's reliability objectives described in the Implementation Guidance could easily consume scores, if not hundreds, of staff hours, with the potential to make "vendor risk assessment(s)" a significant cost component of any large-scale procurement. N&ST notes that although most of the documents referenced in the Guidance document are available for download at no charge, the Shared Assessment Program's Standardized Information Gathering (SIG) questionnaire, referenced in a footnote, must be purchased for $6,000. The Guidance document does point out that a Responsible Entities are free to pursue different approaches to CIP-013 implementation that "better fit their situation," but provides no examples of alternatives that might be worth considering. N&ST encourages NERC and the SDT to consider how utilities with very small staffs and very limited budgets might reasonably address their CIP-013 obligations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Wendy Center - U.S. Bureau of Reclamation - 5	
Answer	No
Document Name	
Comment	
Reclamation's position is that the determination of "cost effectiveness" will remain subjective unless a method to determine burden is consistent across the industry.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Alex Ybarra - Public Utility District No. 2 of Grant County, Washington - 5	

Answer	No
Document Name	
Comment	
There is not enough clarity in the proposed language to make that assessment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Patricia Robertson - BC Hydro and Power Authority - 1, Group Name BC Hydro	
Answer	No
Document Name	
Comment	
BC Hydro does not agree that implementing this standard will be cost effective. Costs and contract management to enforce CIP-013 on all vendors, in light of the limited authority the responsible entity would have over vendors, are anticipated to be significant. Especially, but not limited too, in situations where there is limited vendor choice for a class of product.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Michael Haff - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	No

Document Name	
Comment	
The Implementation Guidance only identifies items that could be evaluated in developintg a Supply Chain Cyber Security program, but does not provide an example or guidance on how to implement the program. Without this guidance, it is impossible to understand how to comply with CIP-013-1 in a cost-effective and compliant manner.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Shawn Abrams - Santee Cooper - 1	
Answer	No
Document Name	
Comment	
Santee Cooper believes that this standard will increase the cost of purchasing products from vendors unless the standard effectively addresses the use of regional master contracts, master agreements, and piggyback agreements. If a Responsible Entity loses the ability to utilize such contracts and agreements the aggregated buying power and large purchase discounts will be lost.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	No

Document Name	
Comment	
CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity. Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities. The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., "Each Responsible Entity shall <insert performance activity> and document the results of the assessment."). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	No
Document Name	
Comment	

By not clarifying “cyber security risks” in R1 Part 1.1 the SDT is not providing flexibility, but rather compliance risk to Registered Entities. See our comments to questions 1 and 7, above, regarding the Implementation Guidance. As it stands, the document provides no guidance and raises additional, possible compliance risk as to interpretation of what “cyber security risks” are.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	No
Document Name	
Comment	
CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity. Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities. The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments.	
Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	No
Document Name	
Comment	

CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall <insert performance activity> and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	

Answer	No
Document Name	
Comment	

CHPD believes that the language proposed in CIP-013-1 Draft 2 will result in vendor costs that outweigh, or possibly reverse, the current security and reliability of the BES. Vendors are likely to (1) significantly increase quoted implementation costs, (2) counter terms with alternate language that may not comply with the Standard, or (3) elect to no longer do business with small-to-medium sized entities due to added contractual complexity.

Vendors are not subject to enforcement and therefore should not be identified in any CIP Standards. As a result, CHPD proposes that the requirements be written in a less prescriptive manner that enables entities responsible for CIP-013 compliance to have control over the process through the use of performance-based activities.

The performance-based assessment requirements would be improved if worded in a way that allows the acceptance of any outcome reached by each Responsible Entity (e.g., “Each Responsible Entity shall and document the results of the assessment.”). The intent should be to create a dialog between the entities and vendors on these topics rather than just documented within contractual language.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Richard Vine - California ISO - 2

Answer	Yes
Document Name	
Comment	

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bradley Calbick - Bradley Calbick On Behalf of: Bryan Cox, Avista - Avista Corporation, 3, 1, 5; - Bradley Calbick	
Answer	Yes
Document Name	
Comment	
Avista agrees with the SDT's belief that the proposed CIP-013-1 and the ERO Enterprise-Endorsed Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements. In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	

ERCOT joins the comments of the IRC.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	Yes
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	Yes
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	Yes
Document Name	
Comment	

No comment.	
Likes 0	
Dislikes 0	
Response	
Timothy Reyher - Eversource Energy - 5	
Answer	Yes
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	Yes
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	

Dislikes 0	
Response. Thank you for your comments.	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	Yes
Document Name	
Comment	

We support the changes and believes that most aspects of CIP-013 may be achieved cost-effectively (if not necessarily cheaply), with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, USI strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. USI suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 1	Chris Gowder, N/A, Gowder Chris
Dislikes 0	

Response. Thank you for your comments.	
David Rivera - New York Power Authority - 3	
Answer	Yes
Document Name	
Comment	
NYPA supports the comments submitted by Salt River Project (WECC) and NPCC.	
Likes 0	
Dislikes 0	
Response	
Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI agrees with the SDT's belief that the proposed CIP-013-1 and the ERO Enterprise-Endorsed Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements. In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements.	

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	Yes
Document Name	
Comment	
In the Draft CIP-013-1 – Cyber Security - Supply Chain Risk Management requirement R2 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." With this note the Responsible Entity is basically directed to develop a plan yet it does not have to change procurement results. If you are not going to require results, there is no reason to add the costs of developing and implementing the program.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Andrey Komissarov - Andrey Komissarov On Behalf of: Jerome Gobby, Sempra - San Diego Gas and Electric, 5, 3, 1; - Andrey Komissarov	
Answer	Yes
Document Name	
Comment	

SDG&E is not able to determine if the proposed CIP-013-1 and the draft Implementation Guidance are cost effective. Additional changes to existing contracts could incur significant cost increases.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	

SRP generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, SRP strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BCS. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. SRP suggests that the option for a Technical Feasibility Exception be allowed for legacy

systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	Yes
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
See attached comments.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Andrew Gallo - Austin Energy - 6	
Answer	Yes
Document Name	
Comment	
AE generally agrees the entities can meet the reliability objectives in a cost effective manner with two exceptions:	

(1) One exception is if the audit approach to CIP-013 effectively precludes use of regional master contracts and "piggyback" agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for: (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place of pre-negotiated master agreements, and (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, AE strongly urges that audit approach language for CIP-013 R2 be clarified to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors. (2) Implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BCS. Some legacy cyber systems are inherently structured and configured for vendor access and reworking them to allow real-time changes may degrade system performance. AE suggests the option for a Technical Feasibility Exception be allowed for legacy systems or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Joe Tarantino - Joe Tarantino On Behalf of: Arthur Starkovich, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Beth Tincher, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Jamie Cutlip, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Kevin Smith, Balancing Authority of Northern California, 1; Lori Folkman, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; Susan Oto, Sacramento Municipal Utility District, 4, 1, 5, 6, 3; - Joe Tarantino	
Answer	Yes
Document Name	
Comment	

SMUD generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, SMUD strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. SMUD suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Harold Sherrill - Harold Sherrill On Behalf of: Martine Blair, Sempra - San Diego Gas and Electric, 5, 3, 1; - Harold Sherrill

Answer	Yes
Document Name	

Comment

SDG&E is not able to determine if the proposed CIP-013-1 and the draft Implementation Guidance are cost effective. Additional changes to existing contracts could incur significant cost increases.

Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Tyson Archie - Platte River Power Authority - 5	
Answer	Yes
Document Name	
Comment	

PRPA generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if the eventually determined audit approach to CIP-013 effectively precludes use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other public utilities with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually in place in pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, PRPA strongly urges that audit approach language for CIP-013 R2 be clarified as to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions and auditors.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. PRPA suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

Likes 0	
Dislikes 0	

Response. Thank you for your comments.	
Allan Long - Memphis Light, Gas and Water Division - 1	
Answer	Yes
Document Name	
Comment	
We support APPA's submitted comments regarding the cost-effectiveness of CIP-013, pointing out two exceptions.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	Yes
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	
Response	
Aaron Ghodooshim - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6 - RF, Group Name FirstEnergy Corporation	

Answer	Yes
Document Name	
Comment	
Note – Comments from EEI follow: "EEI agrees with the SDT's belief that the proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. However, the cost effectiveness of the standard will ultimately depend on how Responsible Entities implement the standard and how NERC and the Regional Entities enforce the requirements. In addition to the Implementation Guidance, the policy guidance that NERC staff and the Standards Committee are drafting to clarify the principles, development, and use of the Guidelines and Technical Basis will also be very important to how Responsible Entities implement the requirements. "	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Jeff Icke - Colorado Springs Utilities - 5	
Answer	Yes
Document Name	
Comment	
Colorado Springs Utilities supports the comments provided by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

Steven Rueckert - Western Electricity Coordinating Council - 10	
Answer	Yes
Document Name	
Comment	
WECC concurs the draft of CIP-013-1 and the draft Implementation Guidance provide the flexibility sought by industry in its collective comments to the first ballot.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Bob Thomas - Illinois Municipal Electric Agency - 4	
Answer	Yes
Document Name	
Comment	
Illinois Municipal Electric Agency supports comments submitted by the American Public Power Association.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	

Answer	Yes
Document Name	
Comment	
Implementing action plans to meet reliability objectives should be cost effective, but cost effectiveness is different for each entity. Reasonable expectations of what's determined as "cost effectiveness" should be considered on an individual utility/entity basis.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Glen Farmer - Avista - Avista Corporation - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Brandon Cain - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rhonda Bryant - El Paso Electric Company - 3	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Pablo Onate - El Paso Electric Company - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Victor Garzon - El Paso Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
IESO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sergio Banuelos - Tri-State G and T Association, Inc. - 1,3,5 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

David Ramkalawan - Ontario Power Generation Inc. - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Stephanie Little - Stephanie Little	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Quintin Lee - Eversource Energy - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jesus Sammy Alcaraz - Imperial Irrigation District - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mark Holman - PJM Interconnection, L.L.C. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Allie Gavin - Allie Gavin On Behalf of: Michael Moltane, International Transmission Company Holdings Corporation, 1; - Allie Gavin	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
David Gordon - Massachusetts Municipal Wholesale Electric Company - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 3	
Answer	Yes

Document Name	
Comment	
Likes 1	Tallahassee Electric (City of Tallahassee, FL), 1, Langston Scott
Dislikes 0	
Response	
Tho Tran - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Julie Hall - Entergy - 6, Group Name Entergy/NERC Compliance	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Lauren Price - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Thomas Foltz - AEP - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Shelby Wade - PPL - Louisville Gas and Electric Co. - 1,3,5,6 - SERC,RF, Group Name PPL NERC Registered Affiliates	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Val Ridad - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Sandra Pacheco - Silicon Valley Power - City of Santa Clara - 3,5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Bill Watson - Old Dominion Electric Coop. - 3	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Randy Buswell - VELCO -Vermont Electric Power Company, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	
No comment	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	

Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	
MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	
Chris Scanlon - Exelon - 1	

Answer	
Document Name	
Comment	
At this point of the project, it is too early to comment on cost effectiveness. Exelon does not predict that the implementation of CIP-013 will require significant investment. However, implementing tools and processes for the revisions to CIP-005 and CIP-010 may require project management oversight as well as material financial investment.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments.	

9. Provide any additional comments for the SDT to consider, if desired.
Mark Holman - PJM Interconnection, L.L.C. - 2
Answer
Document Name
Comment
The current version of the cybersecurity supply chain standard provides a starting point for advancing controls to mitigate the risks associated with vulnerabilities in the supply chain. PJM Interconnection, LLC ("PJM") is supportive of this proposed standard as a first step consistent with the overall direction provided by the FERC. *PJM wishes to point out that the proposed supply chain standard needs to further evolve through subsequent iterations based on additional experience and incorporation of best practices. Although PJM recognizes the limits of FERC's jurisdiction as it relates to*

suppliers to owners and operators of the bulk electric system, any effective supply chain management standard should work to create incentives for improved cybersecurity practices up the supply chain and not just place requirements on the end user (in this case the owner or operators of bulk electric system assets). Although not evident on its face, PJM is hopeful that the proposed Standard will adequately and timely incent that goal. However, as a first step, the impact of the proposed standard, once implemented, should be analyzed with this goal in mind.

In order for supply chain risks to be substantially mitigated it will require broader cross sector engagement, broad government engagement and a significant shift in how vendors and service providers deliver products and services. Broader engagement is also required to ensure an equitable allocation of liabilities and costs. Eventually vendors and service providers will differentiate themselves by how well they manage cybersecurity risks and meet these customer needs in a fair and responsible manner.

Directionally, the proposed cybersecurity supply chain standard was intended to address a broad range of technologies as opposed to a narrower view of Energy Management and Market Management System vendors. The FERC directive similarly appeared to drive this approach. By making this choice of applying the standard to a broader range of technologies the standard, almost by necessity, starts with a more general approach with is not overly prescriptive and is grounded on the principle that organizations must establish cybersecurity supply chain processes and then execute against those processes.

The standard could have been much more prescriptive had it taken a narrower approach focusing primarily on SCADA Systems, Energy Management Systems, and Market Management Systems software solutions. Clearly the more narrow approach would have allowed for additional focus on those systems most critical to ISO/RTO operations where more proscription could have been helpful to drive more specific cybersecurity controls up the supply chain. Whether a broad approach as chosen by the drafting team or a more targeted approach is better as a starting place can be legitimately debated. In any event, either can provide a starting point for making improvements in managing the cybersecurity supply chain threats. PJM believes this effort meets that initial 'out of the gate' requirement given the need for compliance with the FERC Order in a discrete time period.

Support of the cybersecurity supply chain standard will provide an incremental step in achieving our objective of significantly improving the risks associated with vulnerabilities in the supply chain.

Likes 0	
Dislikes 0	

Response. Thank you for your comments.

Brenda Hampton - Luminant - Luminant Energy - 6, Group Name Luminant	
Answer	
Document Name	
Comment	
Luminant wants to thank the Supply Chain SDT for their diligence in reviewing the previous comments and using those comments to appropriately craft the current proposed documents. Luminant also wants to encourage the SDT to review the comments submitted during this ballot period and consider changes to the standards, as appropriate, even if these standards are passed by the ballot body.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT believes the proposed changes in the next posting are responsive to stakeholder comments, improve the quality of the standards, and meet the directives in Order No. 829.	
Linda Jacobson-Quinn - City of Farmington - 3	
Answer	
Document Name	
Comment	
FEUS supports the comments submitted by APPA	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Scott Downey - Peak Reliability - 1	
Answer	
Document Name	
Comment	
Peak Reliability believes the proposals are a step in the right direction but as written do not provide the value intended.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Michael Shaw - Lower Colorado River Authority - 6, Group Name LCRA Compliance	
Answer	
Document Name	
Comment	
1) Make 'vendor' a defined term or provide GTB explanation for what is expected to be considered a vendor. 2) Guidelines and Technical Basis for CIP-013-1 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems can a reliable software update source be identified once? 3) Please provide implementation guidance on CIP-005 and CIP-010 4) Make 'integrity' a defined term or provide GTB explanation for what is expected for verifying integrity of software. 5) Please list practical ways to validate the integrity of software.	

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has addressed the comments in previous sections.	
Wesley Maurer - Lower Colorado River Authority - 5	
Answer	
Document Name	
Comment	
Make 'vendor' a defined term or provide GTB explanation for what is expected to be considered a vendor. Guidelines and Technical Basis for CIP-013-3 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems can a reliable software update source be identified once? Please provide implementation guidance on CIP-005 and CIP-010 Make 'integrity' a defined term or provide GTB explanation for what is expected for verifying integrity of software. Please list practical ways to validate the integrity of software.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has addressed the comments in previous sections.	
Michael Brytowski - Michael Brytowski On Behalf of: Donna Stephenson, Great River Energy, 5, 3, 1, 6; - Michael Brytowski	
Answer	

Document Name	
Comment	
GRE appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Timothy Reyher - Eversource Energy - 5	
Answer	
Document Name	
Comment	
No Cooent	
Likes 0	
Dislikes 0	
Response	
Warren Cross - ACES Power Marketing - 1,3,4,5 - WECC,Texas RE,SERC,SPP RE,RF, Group Name ACES Standards Collaborators	
Answer	
Document Name	
Comment	

: The SDT doesn't address CIP Exceptional Circumstance (CEC) in any of the Supply Chain Standards. If an event does occur that creates a CEC, it could potentially cause an entity to not be able to monitor vendor remote access verification of software integrity and authenticity.

In Order No. 829, it states, "new or modified 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."

Does the drafting team have confidence that only having in scope medium and high BES Cyber Assets meets the directive for "industrial control system hardware, software, and services"?

ACES recommends additional verbiage be written in the requirements to document what cyber assets that are not in scope for Supply Chain Management such as: Electronic Access Control and Monitoring Systems (EACMS), transient cyber assets, removable media and protected cyber assets (PCA).

Thank you for your time and consideration.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

The SDT does not believe the proposed requirements need to include exceptions for CIP Exceptional Circumstances as discussed in previous sections.

The SDT believes the scope is appropriate, as discussed in response to Question 7.

The SDT does not believe it is necessary to expand on the list of exemptions; rather, the SDT has included the applicability in the appropriate section of the standard, and in the requirements themselves. This approach is consistent with other Reliability Standards.

Theresa Rakowsky - Puget Sound Energy, Inc. - 1	
Answer	
Document Name	
Comment	
PSE supports comments submitted by EEI.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name RSC no Dominion	
Answer	
Document Name	
Comment	
No comment	
Likes 1	Chantal Mazza, N/A, Mazza Chantal
Dislikes 0	
Response	
Jason Snodgrass - Georgia Transmission Corporation - 1	
Answer	
Document Name	

Comment	
GTC appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
David Francis - SRC - 1,2 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF, Group Name SRC + SWG	
Answer	
Document Name	
Comment	
The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches." The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit. Therefore, the IRC suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IRC suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has revised the section in CIP-010-3 to remove the ambiguous material.	

IESO	
Answer	YES
Document Name	
Comment	

There appears to be inconsistency between the requirement and the Guidelines in CIP-010 R1.

The requirement states “For 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”.

The Guidelines and Technical Basis section heading Software and Authenticity, paragraph three on page 39, states: “It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.”

The requirement wording suggests it applies for any change but the guidance suggests that for some changes, such as patches, it would not apply. As the requirement is auditable and the guidance is not, the guidance becomes superfluous. The Guideline also introduces significant ambiguity that is impossible to audit.

Therefor the IESO suggest that either the requirement wording be adjusted to allow for automated patching solutions or the Guideline be removed as it is contradictory. The IESO suggest that automated patch deployment solutions should be able to verify the identity and integrity of the patch. Therefore the best solution is to remove the guideline.

Note: the following comment is the same as identified for question 2.

We note there is no corresponding “Guidance and Technical Basis” or “Rationale” for CIP-005-6 Requirement R2 Parts 2.4 and 2.5.

Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT has revised the section in CIP-010-3 to remove the ambiguous material. Also, see response in Question 2.	
Teresa Cantwell - Lower Colorado River Authority - 1	
Answer	
Document Name	
Comment	
1. Make 'vendor' a defined term or provide GTB explanation for what is expected to be considered a vendor. 2. Guidelines and Technical Basis for CIP-013-3 states that it is sufficient to establish a reliable software update source once to allow automated solutions to be implemented. Does this reasoning extend to manual patching? For non-automated systems, can a reliable software update source be identified once? 3. Please provide implementation guidance on CIP-005 and CIP-010. 4. Make 'integrity' a defimed term or provide GTB explanation for what is expected for verifying integrity of software. 5. Please list practical ways to validate the integrity of software.	
Likes 0	
Dislikes 0	
Response Thank you for your comment. See response in previous sections.	
William Harris - Foundation for Resilient Societies - 8	
Answer	

Document Name	Resilient Societies Comments - NERC Cyber Supply Chain Risk Management 2016-03.docx
Comment	
See combined comments of the Foundation for Resilient Societies in the attached file. (Comment at end of document)	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.

1. The proposed standards will benefit reliability and enhance the existing body of CIP Reliability Standards by addressing supply chain cyber security risks to applicable medium and high impact BES Cyber Systems. The effort is in recognition of the significant and evolving threats to the cyber security of BES Cyber Systems in the supply chain. The proposed standards are responsive to FERC Order No. 829 and support a defense-in-depth strategy by adding planning and procurement obligations to "post-acquisition activities at individual entities" (Order No. 829, P. 34).
2. The proposed standards address the four supply chain cyber security objectives in Order No. 829 (software integrity and authenticity; vendor remote access; information system planning; and vendor risk management) through requirements for responsible entities to implement various planning and procurement processes and operating measures. Consistent with the Order, the proposed standards provide responsible entities with flexibility to determine how to meet the reliability objectives (Order No. 829, P. 2). Flexibility is needed due to the diverse population of responsible entities, the variety of systems and services covered by the standards, entity and vendor-specific procurement processes involved, and the evolving nature of cyber security supply chain risks and mitigation.
3. The proposed standards and Order No. 829 directing their development are informed by pertinent threat advisories and information (Order No. 829, P. 26). As discussed above, the proposed requirements provide entities with flexibility for achieving the objectives and avoid prescriptive measures that may not provide reliability benefits or deliver the most efficient or effective approach. Instead, the standards and Implementation Guidance reference current technical guidance where appropriate.
4. The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. See response to Question 4 comments. Security of communications is not in scope for this project.

5. As discussed above, the proposed standards support a defense-in-depth strategy by adding planning and procurement obligations for responsible entities to other CIP cyber security practices. The SDT's approach is in line with FERC Order No. 829, which stipulates that the standards should not impose obligations directly on vendors (Order No. 829, P 36). 6. The SDT is addressing the concern with potentially varying compliance interpretations by developing Implementation Guidance. The ERO Enterprise has endorsed the CIP-013-1 Implementation Guidance in accordance with NERC's Compliance Guidance policy. As a result, responsible entities have a vetted example of a compliant approach to support compliance monitoring activities. 7. Approved CIP standards contain requirements for mitigating malicious code and reporting cyber security incidents. Project 2016-03 is focused on the objectives contained in the project Standard Authorization Request and Order No. 829.

John Martinsen - Public Utility District No. 1 of Snohomish County - 4	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Long Duong - Public Utility District No. 1 of Snohomish County - 1	
Answer	
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Mark Oens - Snohomish County PUD No. 1 - 3	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Sam Nietfeld - Public Utility District No. 1 of Snohomish County - 5	
Answer	
Document Name	
Comment	

Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Franklin Lu - Snohomish County PUD No. 1 - 6	
Answer	
Document Name	
Comment	
Public Utility District No. 1 of Snohomish County supports the comments of Seattle City Light, Salt River Project and New York Power Authority – LPPC members.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Elizabeth Axson - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	

ERCOT joins the comments of the IRC and offers the following additional comment:

The term "vendor" that is used repeatedly in the rationale boxes requires further clarification or revision. "A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."

Services cannot be manufactured, and the provision of services is already addressed through item (ii). ERCOT suggests the following revision: "A *vendor*, as used in the standard, may include: (i) developers or manufacturers of information systems or components; (ii) *providers of information systems services*; (iii) product resellers; or (iv) system integrators."

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT believes the vendor description as written provides responsible entities with the necessary context to meet the requirements.

Richard Vine - California ISO - 2

Answer	
Document Name	

Comment

The ISO supports the comments of the Security Working Group (SWG)

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

Brian Millard - Tennessee Valley Authority - 1,3,5,6 - SERC, Group Name Tennessee Valley Authority	
Answer	
Document Name	
Comment	
Regarding requirement R2, measure M2, suggest consider revising language to state "…demonstrate use of ***or compliance with*** *the supply chain cyber security risk management plan."*	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT does not believe the suggested change provides additional clarity.	
Janis Weddle - Public Utility District No. 1 of Chelan County - 6	
Answer	
Document Name	
Comment	
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Haley Sousa - Public Utility District No. 1 of Chelan County - 5	
Answer	
Document Name	
Comment	
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chad Bowman - Public Utility District No. 1 of Chelan County - 1	
Answer	
Document Name	
Comment	
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.	
Likes 0	
Dislikes 0	

Response. Thank you for your comment.	
Sean Bodkin - Dominion - Dominion Resources, Inc. - 6, Group Name Dominion	
Answer	
Document Name	
Comment	

Dominion recommends the following changes to the RSAWs:

- CIP-005-6, R2, Parts 2.4 and 2.5
  - Remove the word “all” from the “Compliance Assessment Approach sections.
- CIP-010-3, R1, Part 1.6
  - Remove the words “for each” from the “Compliance Assessment Approach section, rows 2 and 4.
- CIP-013-1, R1
  - Remove the word “controls”. The word “processes” is now in uses in the most current draft of CIP-013-1.

Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will provide this feedback to the RSAW Task Force for consideration.	
Mick Neshem - Public Utility District No. 1 of Chelan County - 3	
Answer	
Document Name	

Comment
CHPD sees value in broader engagement by other governmental authorities, including potentially the Department of Homeland Security and the Department of Energy, in order to address electric sector supply chain security in a manner that fully engages responsible suppliers with whom we do business. That effort could lead to an articulated set of common practices or protocols to which entities in the electric supply chain may subscribe, and upon which the electric sector may rely to improve the security of the supply chain.

Likes 0	
Dislikes 0	

Response. Thank you for your comment.

Patrick Hughes - National Electrical Manufacturers Association - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	NEMA Comments on NERC Supply Chain Risk Management 2017-06-12.pdf

Comment
On behalf of the National Electrical Manufacturers Association (NEMA)—a trade association and standards developing organization with nearly 350 member companies that manufacture a diverse set of products used in the generation, transmission, distribution, and end-use of electricity—and on behalf of the NEMA Grid Modernization Leadership Council and the NEMA Cybersecurity Committee, I wish to submit for your reference "CPSP 1-2015: Supply Chain Best Practices," which describes industry best practices for manufacturers to follow regarding cybersecurity supply chain management. "Supply Chain Best Practices" identifies guidelines that electrical equipment manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses or other exploits can be used can be used to negatively impact product operation. It addresses United States supply chain integrity through four phases of a product's life cycle: manufacturing, delivery, operation, and end-of-life. The report (attached) is available for public download at: http://www.nema.org/Standards/Pages/Supply-Chain-Best-Practices.aspx.

The National Electrical Manufacturers Association and its members understand that a secure supply chain is essential to a secure grid and that cybersecurity aspects should be built into, not bolted onto, manufacturers' products. They also understand that managing cybersecurity supply chain risk requires a collaborative effort and open lines of communication among electric utility companies and the manufacturers of critical electric grid systems and components—both hardware and software. NEMA looks forward to working with and being a resource for NERC, utilities, and other interested stakeholders in addressing supply chain risks and concerns within the energy sector. Should you have any questions, please contact Patrick Hughes, Senior Director of Government Relations and Strategic Initiatives, at 703-841-3205 or patrick.hughes@nema.org. Respectfully, Kyle Pitsor Vice President, Government Relations	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Steven Sconce - EDF Renewable Energy - 5	
Answer	
Document Name	
Comment	
No comment.	
Likes 0	
Dislikes 0	

Response	
Louis Guidry - Louis Guidry On Behalf of: John Lindsey, Cleco Corporation, 6, 5, 3, 1; Michelle Corley, Cleco Corporation, 6, 5, 3, 1; Robert Hirchak, Cleco Corporation, 6, 5, 3, 1; Stephanie Huffman, Cleco Corporation, 6, 5, 3, 1; - Louis Guidry	
Answer	
Document Name	
Comment	
The Guidance and Techincal Basis section is empty.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. See the Implementation Guidance.	
Thomas Foltz - AEP - 5	
Answer	
Document Name	
Comment	
AEP urges the SDT to consider FERC Order 706 paragraph 355 which requires a policy for each of the cyber security topical areas. CIP-003 R1 should require a policy for supply chain cyber security.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will provide this information to the CIP Modifications SDT.	

Tyson Archie - Platte River Power Authority - 5	
Answer	
Document Name	
Comment	
Platte River Power Authority also supports the comments submitted by the American Public Power Association (APPA)	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Amelia Sawyer - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	
Document Name	
Comment	
CenterPoint Energy appreciates the Standard Drafting Team's thorough consideration of comments. Although some concerns with implementation remain, CenterPoint Energy believes that the revisions have made the draft Standard focused and risk-based. CenterPoint Energy also commends the coordination with the CIP Modifications team to place certain requirements appropriately in the body of the existing CIP Standards. Thank you for your efforts.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Andrew Gallo - Austin Energy - 6	

Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Ginette Lacasse - Seattle City Light - 1,3,4,5,6 - WECC, Group Name Seattle City Light Ballot Body	
Answer	
Document Name	2016-03_Unofficial_Comment_Form_SCL_2017-6-14 Final to NERC.docx
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Normande Bouffard - Hydro-Quebec Production - 5	
Answer	
Document Name	
Comment	

No comment	
Likes 0	
Dislikes 0	
Response	
Lona Calderon - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Alan Farmer - ACEC - NA - Not Applicable - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	

The American Council of Engineering Companies (ACEC) -the business association of the nation's engineering industry - wants to convey the industry's perspectives and concerns over the development of this new cyber security supply chain rule mandated by the Federal Energy Regulatory Commission (FERC). ACEC members firms, numbering more than 5,000 and representing over 500,000 employees throughout the country, are engaged in a wide range of engineering work that propel the nation's economy, and enhance and safeguard America's quality of life. Council members are actively involved in every aspect of the energy marketplace. Supply chain cyber security is of growing concern to all our members. ACEC is in agreement with most of the comments of the owners, operators, vendors and suppliers that have formally participated in this Standard development.

Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Barry Lawson - National Rural Electric Cooperative Association - 4	
Answer	
Document Name	
Comment	
NRECA appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	

Melanie Seader - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	
EEI greatly appreciates the work of the SDT and NERC in reviewing and addressing stakeholder feedback from the first ballot. EEI supports the currently posted drafts and ask that the SDT look to our members' individual comments for further suggestions for improvement.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
David Rivera - New York Power Authority - 3	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Russel Mountjoy - Midwest Reliability Organization - 10, Group Name MRO NSRF	
Answer	

Document Name	
Comment	
Please note that the NSRF has concerns with the Webinar and Guidance going outside of the scope of the proposed Requirements. All applicable entities will need to satisfy the Requirements once approved by FERC per FERC Order 693, setcion253. Regardless of what the Webinar or Guideline states.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Chris Scanlon - Exelon - 1	
Answer	
Document Name	
Comment	
None.	
Likes 0	
Dislikes 0	
Response	
Brian Evans-Mongeon - Utility Services, Inc. - 4	
Answer	
Document Name	

Comment	
No comment	
Likes 0	
Dislikes 0	
Response	
Guy Andrews - Georgia System Operations Corporation - 4	
Answer	
Document Name	
Comment	
GSOC appreciates the work and efforts of the SDT.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Scott Miller - Scott Miller On Behalf of: David Weekley, MEAG Power, 3, 5, 1; Roger Brand, MEAG Power, 3, 5, 1; Steven Grego, MEAG Power, 3, 5, 1; - Scott Miller, Group Name MEAG Power	
Answer	
Document Name	
Comment	

MEAG supports the answers and comments of Salt River Project.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Kara White - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	

Additional comments received from Seattle City Light

1. The SDT has revised requirements for developing and implementing supply chain cyber security risk management plans (CIP-013-1 Requirements R1 – R3) in response to stakeholder comments. Do you agree with the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the proposed requirements, please provide your recommendation and explanation.

☒ Yes
☐ No

Comments: *Note that for all comments (1-9) written in blue text come directly from APPA and/or LPPC comments. Any comments in black are City Light's.*

Seattle City Light continues to be a strong supporter of efforts to ensure the security of the Bulk Electric System and appreciates the time and effort that the SDT has put into considering industry feedback and incorporating it into the current drafts of CIP-005, CIP-010 and CIP-013.

Seattle agrees with limiting the requirement to high and medium assets only.

R1: Seattle generally agrees with the proposed Requirement 1 but is concerned about compliance obligations for procurement activities associated with multi-party wide-area contracts, master agreements and piggyback agreements. An exception, comparable to a CIP Exceptional Circumstance, might be included in the standard for these kinds of procurement activities. Alternatively, concerns about how different type of contracts—multi-party contracts, master agreements, evergreen agreements, piggyback contracts, long-term service agreements, etc, etc, etc—may or may not comply might be addressed by re-positioning CIP-013 as a performance-based Standard, with a focus on managing specific aspects of vendor security rather than particular contracting practices.

Our reasoning is that there are means other than vendor contract negotiations, contract language, and procurement processes to address and (attempt to) achieve the protections identified in R1.2. It is immaterial how these protections are pursued. Focusing vendor security plans and audit approaches on contracts and procurement (even if specific contract terms are not in scope) limits flexibility, is unnecessarily prescriptive, and does not reflect performance-based principles. As such we suggest that R1.2 be revised as follows:

> ***1.2.*** *One or more process(es) for its newly procured BES Cyber Systems that address the following elements, as applicable:*

As explanation for the revisions, underlined words are added, and "newly" is intended to mean 'obtained after the implementation of CIP-013.' Also, the term "elements," as shown above, is added to more clearly align with the VSLs for this requirement.

At the same time guidance associated with the "Rationale for R1," "Rationale for R2," and the separate Implementation Guidance document should be revised to reflect the change to a performance-based requirement in which contract terms and contract negotiations play no necessary function in vendor security plans and audit approaches. Contract terms might be used by an entity in their vendor security plans and/or as evidence of performance, but there should be no expectation by auditors or subtext in the Standard or Implementation Guidance that anything having to do with contracts or procurement processes is required. There should be no expectation of what might or should be included within Requests for Proposals, no expectation of when contracts might or should be renegotiated, no expectations of what contract terms might or should be included or requested, and no expectations of what terms might or should be found in a prudent and proper contract. Ultimately there should be no expectation that CIP-013 R1.2 protections be achieved through the contracting process. Consistent with performance-based standard principles the objective in CIP-013 and in entity vendor security plans should be on achieving each protection (as feasible), not on the means by which it is achieved (or attempted to be achieved).

In the absence of such changes, we request substantial additional clarification about how, without contract terms and contract negotiations being auditable, performance of R2 implementation will be audited and assessed. In particular for state and regional master agreements, piggyback contracts, evergreen agreements, and the like.

Looking to specific details of CIP-013 requirements, Seattle requests re-wording of R1 parts 1.2.1 and 1.2.4 to better understand what is expected. These parts appear to be duplicative. The endorsed Guidance does not adequately distinguish between the two parts. One interpretation is that part 1.2.1 is for products/services and that part 1.2.4 is for vulnerabilities in the product. It is not clear if these parts expect information sharing at the time of procurement or if information sharing will be on-going?

In R1 parts 1.2.1 and 1.2.2, the term "vendor-identified incident" is unclear. It could mean incidents that were identified by another party, specific to the products of a specific vendor, or incidents identified by the vendor. Seattle suggests changing "identified" in the phrase, to "acknowledged" or "confirmed" to ensure clarity.

Definition of vendor is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005.

Seattle believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that entities include their definition of "vendor" in their plan(s).

Seattle recommends removing those items (CIP-013 R1 parts 1.2.5 and 1.2.6) covered in CIP-005 and CIP-010 from CIP-013 to avoid duplication. The revised CIP-013 parts 1.2.5 and 1.2.6 appear to apply to software source and identity verification (now required "when the method to do so is available" by CIP-010) and determining active vendor remote access sessions (now required by CIP-005). Having CIP-013 parts that require entities to perform the underlying function and to take those functions into account during the procurement process is needless duplication that does not increase security or reliability and could result in compliance "double jeopardy."

R2: Seattle agrees with the requirement to implement the supply chain cyber security risk management plan as outlined in Requirement 1.

As discussed above, Seattle urges the significant additional guidance, preferably centered on performance-based principles, about expected compliance practices and how implementation will be audited. In particular for state and regional master agreements, piggyback contracts, evergreen agreements, and the like.

Finally, the Compliance and/or Implementation Guidance should make clear that, when evidence demonstrates that all items expressly identified in CIP-013, R1 are contained in a Supply Chain Cyber Security Management Plan or Plans, and are implemented pursuant to R2, entities will not be found out of compliance. More specifically, entities should not be subjected to CIP-013 noncompliance findings resulting from a difference of opinion concerning security adequacy.

R3: Seattle agrees that a 15-month review period is appropriate to review the supply chain cyber security risk management plan in Requirement 1.

Additionally, Seattle proposes that the regional entities voluntarily assess CIP-013 programs for entities who have audits in the period between standard approval and the effective date. This is similar to when the regional entities performed transition period audits of CIP v5 programs.

2. The SDT developed proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5 to address the Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access. The SDT followed

an approach recommended by stakeholders during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-005-6? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

The proposed CIP-005-6 uses the term, "vendor." The definition of vendor is not a NERC defined term. Seattle City Light believes the SDT should provide guidance regarding the use of the term "vendor." If "Vendor" is not defined by NERC, the Guidance should recommend that Entities include their definition of "vendor" in their plan(s).

Seattle agrees with R2 Part 2.4 but requests clarification of the term "determining."

Seattle generally agrees with Proposed R2 Part 2.5 but requests revisions to the Rationale for R2. The last sentence of paragraph 2 of the rationale states the objective "is for entities to have the ability to rapidly disable active remote access sessions…" The Responsible Entity may not have the capability to disable access during an "active" remote access session. Seattle requests changing the language to "upon detected unauthorized activity."

Guideline & Technical Basis (GTB) for R2 should be included in this revision. Supplemental materials may be out of date – see page 21 of 24 in the posted redline version. Please Include reference to FERC Order 829 for parts 2.4 and 2.5.

The SDT should consider adding a CIP Exceptional Circumstance clause to R2 parts 2.4 and 2.5

3. The SDT developed proposed CIP-010-3 Requirement R1 Part 1.6 to address the Order No. 829 directive for entities to address verification of software integrity and authenticity in the BES Cyber System environment (P 48). The SDT followed an approach recommended by stakeholders

during the initial posting of CIP-013-1. Do you agree with proposed revisions in CIP-010-3? If you do not agree, or if you agree but have comments or suggestions for the proposed requirement, please provide your recommendation and explanation.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light agrees this requirement belongs in CIP-010 R1. Seattle generally agrees with Proposed R1 Part 1.6, but request the following items be addressed by the SDT:

- Seattle recommends the Guidelines and Technical Basis section is updated to reflect current information.
  - The requirement states "For 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…," indicating the authenticity and integrity of the specified parts need to be verified each time there is a change to a baseline for those parts. The proposed requirement would possibly involve entities duplicating effort for every case for which such verification had to be undertaken (i.e., in the cases of multiple installations of software across many applicable Cyber Assets). This does not seem consistent with the intent of the protection and could present an undue compliance burden without providing the intended protection. We believe that the existing statement in the GTB provides clarity on this issue and request that it not be removed. From the GTB: "It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches."
  - Seattle also recommends the language of the requirement be re-worded to reflect the intent of the GTB, as an auditor audits to the requirement, not the GTB. Doing a verification of authenticity and integrity for each change to the baseline for the specified parts would be tedious and require entities to acquire additional resources to perform the work.
- There is no guidance on how to verify the identity (authenticity). Performing this verification could be difficult if the software/patch comes from a third-party tool. Guidance on how this can be done needs to be made available to entities in order to perform an evaluation of the work and resources involved to achieve this requirement. Hashing was given as an example during an industry webinar, but this is not realistic for each type of system.
- Additional examples of acceptable measures should to be listed, in particular for R1.6.1 and R1.6.2. Additionally, Seattle requests examples of acceptable evidence when there is not a method available to verify the identity of the software source.
- While Seattle supports these changes, clarification is required about how new R1.6 applies to entirely new BES Cyber Systems (BCS), i.e., BCS that are newly implemented, have not previously had a baseline, and thus do not have an existing baseline for a change to

deviate from. We expect that R1.6 is intended to apply to new BCS as well as to existing BCS, but as written the requirement does not. Please clarify to avoid implementation confusion and minimize audit challenges.

4. The SDT removed low-impact BES Cyber Systems from the applicability in CIP-013-1 and is not proposing any new requirements for these cyber systems. The SDT believes that the proposed applicability to high and medium impact BES Cyber Systems appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations, as specified in Order No. 829. Do you agree with the SDT's removal of low impact BES Cyber Systems from CIP-013-1? If you do not agree, or if you agree but have comments or suggestions, please provide your recommendation and explanation.

☒ Yes
☐ No

Comments: Seattle City Light agrees with the removal of low-impact BES Cyber Systems from CIP-013-1 and agrees that the current standard as written appropriately addresses the Commission's concerns as specified in Order No. 829. Among other things, the Order requests a risk-based approach. Application of Standard CIP-002 is an established, Commission-approved approach to categorize a utility's BES Cyber Systems into high, medium, and low risk classifications. Application of this established risk-based approach to cyber asset procurement for electric utilities is natural, appropriate, and consistent with the guiding CIP philosophy, stated in Section 6 of each CIP Standard, that each Standard "exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational, and procedural controls to mitigate risk to BES Cyber Systems."

Furthermore, Seattle believes that for entities that have a mixture of High, Medium and Low assets, the Low assets would inherently benefit from the additional requirements of Medium and High requirements as a matter of normal business practices. Additionally, many Contracts and Master Agreements are developed for all products and services purchased from a vendor. For Entities that have Low assets only, there would not be additional requirements based on CIP-002 risk based approach, as appropriate to the low BES risk presented by these entities.

Seattle believes that including Lows will require substantial resources by each Responsible Entity to identify and maintain an inventory list of these items, beyond the benefit provided by additional controls. Existing controls inherent to CIP-003 and previous CIP Standards reduce the risk associated with Lows.

5. The SDT revised the Implementation Plan in response to stakeholder comments. Do you agree with the Implementation Plan for the requirements in Project 2016-03? If you do not agree, or if you agree but have comments or suggestions for the Implementation Plan, please provide your recommendation and explanation.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees with an 18-month implementation plan but, would prefer a 24-month implementation plan. Seattle feels that a 24-month timeframe is more appropriate and gives the entity additional time to align budgets and develop processes with vendors and suppliers.

Seattle, in line with our recommendation to move CIP-013 to a performance-based standard as discussed in Question 1 above, also recommends deleting discussion of contracts and contract dates from implementation guidance, and focusing the guidance on BES Cyber Assets procured subsequent to the implementation date of the standard. If performance-based principles are not adopted, Seattle at least asks for clarity to change this General Consideration from:

> *Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.*

To:

> *Supply Chain Risk Management plan must be used by appropriate procurement processes that begin on or after the implementation date.* (Also make corresponding change to the associated note in CIP-013 R2.)

Further, Seattle requests clarification on if/when existing contracts, master contracts, or long-term maintenance agreements that may be re-opened for renegotiation or later put in use (e.g., a state master contract negotiated prior to the CIP-013 implementation date but not actually used by a utility until after CIP-013 implementation date), come into the scope of CIP-013. Seattle notes that shifting to a performance-based Standard, focused on specific vendor protections and not the means that such protections are achieved (i.e., contracts) would minimize the explanations required about such matters.

The Implementation Plan does not handle unplanned changes such as newly identified IROLs or registration changes, etc, that may bring an entity suddenly into scope for CIP-013, CIP-005 R2.4-2.5, and/or CIP-010 R1.6. Seattle therefore requests that the Implementation Plan be modified to address, in a reasonable way, how entities come into compliance if, due to changes, they newly meet applicability at some time after the effective date of the standards.

6. The SDT revised the Violation Severity Levels (VSLs) for requirements in CIP-013-1, CIP-005-6, and CIP-010-3. Do you agree with the Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs) for the proposed requirements? If you do not agree, or if you agree but have comments or suggestions for the VRFs and VSLs, please provide your recommendation and explanation.

☐ Yes
☒ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light agrees with the VRFs and VSLs for CIP-013. As discussed above under Question 1, Seattle requests that the term "elements" be included in CIP-013 R1.2 to clearly align with the VSLs for this requirement.

For CIP-010, Seattle does not find that the VSL covers failures to implement the process. It therefore does not include all possible combinations of violation. Consequently, we request that there be an identified severity level for failure to implement and lower severity levels when a single aspect of the requirements is missing.

For CIP-005, Seattle believes that the VRFs and VSLs should be updated to reflect the same general structure used in CIP-010. The VSL for CIP-005 results in a "Severe" penalty if the entity did not have a method to determine and did not have a method to disable. Seattle would prefer a "High" VSL penalty if the entity has a process to determine but does not have a process to disable, and vice-versa if the entity did not have a process to determine but does have a process to disable.

7. The SDT developed draft Implementation Guidance for CIP-013 to provide examples of how a Responsible Entity could comply with the requirements. The draft Implementation Guidance does not prescribe the only approach to compliance. Rather, it describes some approaches the SDT believes would be effective ways to comply with the standard. See NERC's Compliance Guidance policy for information on

Implementation Guidance. Do you agree with the example approaches in the draft Implementation Guidance? If you do not agree, or if you agree but have comments or suggestions for the draft Implementation Guidance, please provide your recommendation and explanation.

☐ Yes
☒ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees with the Implementation Guidance for CIP-013 and feels that this is a promising new approach but is uncertain if the approach best provides assurance and guidance about these new Standards in the absence of the "Guidance and Technical Basis" sections in each Standard and the intentional flexibility of CIP-013 in particular. Seattle is concerned about the possibilities that NERC and the Regions may withdraw previously-granted endorsement should FERC request revisions to the Standard. As such, Seattle would prefer to see the new "Implementation Guidance Document" supplemented with "Guidance and Technical Basis" sections in each Standard, including for CIP-005-6 R2.4 and R2.5 and for CIP-010-3 R1.6.

As discussed above, "vendor" is not a NERC defined term. The term "vendor" is also used in the proposed CIP-005. Seattle believes the SDT should provide guidance regarding the use of the term "vendor." If "vendor" is not defined by NERC, the Guidance should recommend that entities include their definition of "vendor" in their plan(s).

Neither of the bullets for R3 in the Implementation Guidance sufficiently explain compliance needs because both bullets only deal with plan review and not approval, both of which are necessary for compliance. Therefore, Seattle recommends changing:

"Below are some examples of approaches to comply with this requirement:"

to

"Below is an example of an approach to comply with the review requirement required by: "

In addition, we recommend deleting the following guidance language from the second main bullet, because it is beyond the Requirement and introduced activities that are not explicitly required:

"Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed."

8. The SDT believes proposed CIP-013-1 and the draft Implementation Guidance provide entities with flexibility to meet the reliability objectives in a cost effective manner. Do you agree? If you do not agree, or if you agree but have suggestions for improvement to enable additional cost effective approaches, please provide your recommendation and, if appropriate, technical justification.

☒ Yes
☐ No
Comments: *Note that comments identified in blue text come directly from APPA and/or LPPC comments.*

Seattle City Light generally agrees that the entities can meet the reliability objectives in a cost effective manner for CIP-013-1 with two exceptions.

One exception is if that if, due to uncertainty, anticipated audit risk, an eventually established audit approach, or any other reason, Standard CIP-013 precludes or has a chilling effect on use of regional master contracts and piggyback agreements, then cyber asset procurement expenses will increase for municipal utilities, smaller entities and co-ops, and other publics with little or no benefit. Costs will increase for (i) the procurement process itself, because utilities will need to research specifications and develop contracts individually to replace pre-negotiated master agreements, and for (ii) each purchase, because aggregated buying power and large-purchase discounts will be lost. To minimize these risks, Seattle strongly urges that audit approach language for CIP-013 R2 be clarified in advance to clearly identify the acceptable use of master agreements rather than leave this determination up to individual regions, auditors, time, and chance.

The other exception is the implementation of CIP-005 R2.4 and R2.5 (methods to detect and disable remote access for vendors and vendor system) for existing BES Cyber Systems. Some legacy cyber systems are inherently structured and configured for vendor access, and reworking them to allow real-time detection and, especially, disabling of such access may prove extremely costly. At the same time, these changes may degrade the performance of these systems. Seattle suggests that the option for a Technical Feasibility Exception be allowed for legacy systems, or alternatively that legacy systems be granted an extended implementation period of up to five or ten years (during which such systems likely would be replaced).

9. Provide any additional comments for the SDT to consider, if desired.
Comments: None

End of Seattle City Light Comments

THE FOUNDATION FOR RESILIENT SOCIETIES COMMENTS AS FOLLOWS *ON PROPOSED STANDARD*
2016-03, CYBER SUPPLY CHAIN RISK MANAGEMENT, CIP-005-6, CIP-010-3, AND CIP-013-1:
Filed with NERC June 15, 2017
1. These NERC/SDT attempts to produce a CIP standard for supply chain vulnerabilities fall short in an extreme threat environment. Adversaries' efforts against the electric grid and other civil infrastructure show disdain for U.S. defenses and deep commitment to using Information Operations (including cyber warfare) against the nation. The Bulk Electric System (BES) is a major target—this motivates development of strong capabilities for cyberattack. Adversaries understand full well the dependencies of social and national security institutions and all other critical infrastructures on electric power.

2. There is insufficient substance to the draft standard, other than the usual CIP generalized statements of planning, implementation, and periodic reviews that provide *pro forma* response to FERC Order No. 829. In its 9-1 vote to reject the first draft, the industry sent a clear message to NERC and FERC: the standard requirements are, at present, inadequately defined and therefore the feasibility of cost recovery is hard to judge.

3. Any sincere attempt at compliance with the draft standard requirements by responsible entities will incur high costs with uncertain benefit to the survivability of the BES. The Standard Drafting Team appears to minimize the complexity of the 2014 Russian penetrations of the U.S. BES, its sophisticated multi-layered, years-earlier penetration of vendor's control systems, phishing efforts, firmware modifications, and extensive use of IT vendors' vulnerabilities in operating, communications and networking, and database systems. The draft lacks good protective steps on these vulnerabilities and is therefore inadequate for mitigating risk--especially given the increasing nature of the Russian Havex and BlackEnergy threats evidenced in the follow-on attacks in the Ukraine Grid in 2015 and 2016. Note the recent revelation by ESET and DRAGOS of CRASH OVERIDE malware (associated with the 2016 Ukraine attack) with specific and flexible targeting of "low impact" industrial control systems (ICS). Note also the increasing threat from Distributed Denial of Service (DDoS) IoT and ransomware attacks. To expect several thousand utilities to individually and separately determine self-protective actions under the draft standard is unrealistic. Economies of scale in protection are needed.

4. Exempting "Low Impact" cyber systems leaves vulnerabilities. Also, as Resilient Societies has pointed out on FERC dockets, the exclusion from CIP Standards for all communications and networks between "Electronic Security Perimeters," together with direct internet connectivity to many so-called "low impact" cyber assets, leaves literally thousands of unsecured channels for malware implantation.

5. Stringent application whitelisting/blacklisting and selective third party certification steps, in conjunction with a national deterrence policy, are needed to enhance the minimal-protection from current CIP standards.

6. Ambiguities in standard requirements result in a lack of auditability, as noted by many other commenters.

7. In the short-term, a more practical NERC initiative could be to support a FERC rulemaking to require Bulk Electric System-jurisdictional entities to detect, report, mitigate and remove malware. State PUCs should likewise support a malware mitigation initiative for distribution utilities.

William R. Harris
Foundation for Resilient Societies, Inc.

End of Report

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	May 2 – June 15, 2017

Anticipated Actions	Date
10-day final ballot	July 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Rationale for Requirement R2:
Proposed Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-6 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA		
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5).	Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

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

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	May 2 – June 15, 2017

Anticipated Actions	Date
10-day final ballot	July 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-005 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Rationale for Requirement R2:
Proposed Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement ~~as the objective of Part 2.4~~. The objective of Requirement R2 Part 2.5 is for entities to have the ability to ~~rapidly~~ disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

R2. Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-6 Table R2 –Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-6 Table R2 –Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA		
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access.

CIP-005-6 Table R2 –Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3;~~.~~ OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
			Remote Access and system-to-system remote access) (2.5).	Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	
6	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

CIP-005-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

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

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

A. Introduction

1. **Title:** Cyber Security — Electronic Security Perimeter(s)

2. **Number:** CIP-005-~~5~~6

3. **Purpose:** To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

   4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

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

4.2.3. Exemptions: The following are exempt from Standard CIP-005-~~5~~6:

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

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

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

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

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

5. Effective Dates: See Implementation Plan for Project 2016-03

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

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

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

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

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

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

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

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

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

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

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

- **High Impact BES Cyber Systems with External Routable Connectivity** – Only applies to high impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Medium Impact BES Cyber Systems** – Applies to each BES Cyber Systems categorized as medium impact according to the CIP-002-5 identification and categorization processes.
- **Medium Impact BES Cyber Systems at Control Centers** – Only applies to medium impact BES Cyber Systems located at a Control Center.
- **Medium Impact BES Cyber Systems with Dial-up Connectivity** – Only applies to medium impact BES Cyber Systems with Dial-up Connectivity.
- **Medium Impact BES Cyber Systems with External Routable Connectivity** – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.
- **Electronic Access Points (EAP)** – Applies at Electronic Access Points associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

R1. Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems and their associated: • PCA	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	An example of evidence may include, but is not limited to, a list of all ESPs with all uniquely identifiable applicable Cyber Assets connected via a routable protocol within each ESP.
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	An example of evidence may include, but is not limited to, a list of rules (firewall, access control lists, etc.) that demonstrate that only permitted access is allowed and that each access rule has a documented reason.
1.4	High Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with Dial-up Connectivity and their associated: • PCA	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	An example of evidence may include, but is not limited to, a documented process that describes how the Responsible Entity is providing authenticated access through each dial-up connection.

CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	Electronic Access Points for High Impact BES Cyber Systems Electronic Access Points for Medium Impact BES Cyber Systems at Control Centers	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	An example of evidence may include, but is not limited to, documentation that malicious communications detection methods (e.g. intrusion detection system, application layer firewall, etc.) are implemented.

Rationale for Requirement R2:
Proposed Requirement R2 Parts 2.4 and 2.5 addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES.

The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. This scope covers all remote access sessions with vendors. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. While not required, a solution that identifies all active remote access sessions, regardless of whether they originate from a vendor, would meet the intent of this requirement. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

The scope of Requirement R2 in CIP-005-6 is expanded from approved CIP-005-5 to address all remote access management, not just Interactive Remote Access. If a Responsible Entity does not allow remote access (system-to-system or Interactive Remote Access) then the Responsible Entity need not develop a process for each of the subparts in Requirement R2. The entity could document that it does not allow remote access to meet the reliability objective.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contracts with to supply BES Cyber Systems and related services. It does not include other

NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

R2. Each Responsible Entity ~~allowing Interactive Remote Access to BES Cyber Systems~~ shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].*

M2. Evidence must include the documented processes that collectively address each of the applicable requirement parts in *CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	For all Interactive Remote Access, ~~U~~utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Examples of evidence may include, but are not limited to, network diagrams or architecture documents.
2.2	High Impact BES Cyber Systems and their associated: • PCA	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	An example of evidence may include, but is not limited to, architecture documents detailing where encryption initiates and terminates.

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
	Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA		
2.3	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Require multi-factor authentication for all Interactive Remote Access sessions.	An example of evidence may include, but is not limited to, architecture documents detailing the authentication factors used. Examples of authenticators may include, but are not limited to, • Something the individual knows such as passwords or PINs. This does not include User ID; • Something the individual has such as tokens, digital certificates, or smart cards; or • Something the individual is such as fingerprints, iris scans, or other biometric characteristics.

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	• Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods used to determine active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods for accessing logged or monitoring information to determine active vendor remote access sessions; • Methods for monitoring activity (e.g. connection tables or rule hit counters in a firewall, or user activity monitoring) or open ports (e.g. netstat or related commands to display currently active ports) to determine active system to system remote access sessions; or • Methods that control vendor initiation of remote access such as vendors calling and requesting a second factor in order to initiate remote access. •

CIP-005-~~5~~ 6 Table R2 – ~~Interactive~~ Remote Access Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	High Impact BES Cyber Systems and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).	Examples of evidence may include, but are not limited to, documentation of the methods(s) used to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access), such as: • Methods to disable vendor remote access at the applicable Electronic Access Point for system-to-system remote access; or • Methods to disable vendor Interactive Remote Access at the applicable Intermediate System.

C. Compliance

1. **Compliance Monitoring Process:**

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

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

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

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

   1.3. Compliance Monitoring and Assessment Processes:

   - Compliance Audit
   - Self-Certification
   - Spot Checking
   - Compliance Investigation
   - Self-Reporting
   - Complaint

   1.4. Additional Compliance Information:

   None.

Violation Severity Levels

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-~~5~~ 6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	**Operations Planning and Same Day Operations**	**Medium**			The Responsible Entity did not have a method for detecting malicious communications for both inbound and outbound communications. (1.5)	The Responsible Entity did not document one or more processes for *CIP-005-~~5~~ 6 Table R1 – Electronic Security Perimeter*. (R1) OR The Responsible Entity did not have all applicable Cyber Assets connected to a network via a routable protocol within a defined Electronic Security Perimeter (ESP). (1.1) OR External Routable Connectivity through the ESP was not through an identified EAP. (1.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-~~5~~-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity did not require inbound and outbound access permissions and deny all other access by default. (1.3) OR The Responsible Entity did not perform authentication when establishing dial-up connectivity with the applicable Cyber Assets, where technically feasible. (1.4)
R2.	**Operations Planning and Same Day Operations**	**Medium**	The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3~~;~~ OR	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3~~;~~ OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-005-~~5~~-6)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).	The Responsible Entity did not have one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	1/16/06	R3.2 — Change "Control Center" to "control center."	3/24/06
2	9/30/09	Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3	12/16/09	Updated version number from -2 to -3 Approved by the NERC Board of Trustees.	
3	3/31/10	Approved by FERC.	
4	12/30/10	Modified to add specific criteria for Critical Asset identification.	Update
4	1/24/11	Approved by the NERC Board of Trustees.	Update
5	11/26/12	Adopted by the NERC Board of Trustees.	Modified to coordinate with other CIP standards and to revise format to use RBS Template.
5	11/22/13	FERC Order issued approving CIP-005-5.	

6	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

CIP-005-5-6, Requirement R1 requires segmenting of BES Cyber Systems from other systems of differing trust levels by requiring controlled Electronic Access Points between the different trust zones. Electronic Security Perimeters are also used as a primary defense layer for some BES Cyber Systems that may not inherently have sufficient cyber security functionality, such as devices that lack authentication capability.

All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP. The ESP defines a zone of protection around the BES Cyber System, and it also provides clarity for entities to determine what systems or Cyber Assets are in scope and what requirements they must meet. The ESP is used in:

- Defining the scope of 'Associated Protected Cyber Assets' that must also meet certain CIP requirements.
- Defining the boundary in which all of the Cyber Assets must meet the requirements of the highest impact BES Cyber System that is in the zone (the 'high water mark').

The CIP Cyber Security Standards do not require network segmentation of BES Cyber Systems by impact classification. Many different impact classifications can be mixed within an ESP.

However, all of the Cyber Assets and BES Cyber Systems within the ESP must be protected at the level of the highest impact BES Cyber System present in the ESP (i.e., the "high water mark") where the term "Protected Cyber Assets" is used. The CIP Cyber Security Standards accomplish the "high water mark" by associating all other Cyber Assets within the ESP, even other BES Cyber Systems of lesser impact, as "Protected Cyber Assets" of the highest impact system in the ESP.

For example, if an ESP contains both a high impact BES Cyber System and a low impact BES Cyber System, each Cyber Asset of the low impact BES Cyber System is an "Associated Protected Cyber Asset" of the high impact BES Cyber System and must meet all requirements with that designation in the applicability columns of the requirement tables.

If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. Responsible Entities should know what traffic needs to cross an EAP and document those reasons to ensure the EAPs limit the traffic to only those known communication needs. These include, but are not limited to, communications needed for normal operations, emergency operations, support, maintenance, and troubleshooting.

The EAP should control both inbound and outbound traffic. The standard added outbound traffic control, as it is a prime indicator of compromise and a first level of defense against zero day vulnerability-based attacks. If Cyber Assets within the ESP become compromised and attempt to communicate to unknown hosts outside the ESP (usually 'command and control' hosts on the Internet, or compromised 'jump hosts' within the Responsible Entity's other networks acting as intermediaries), the EAPs should function as a first level of defense in stopping the exploit. This does not limit the Responsible Entity from controlling outbound traffic at the level of granularity that it deems appropriate, and large ranges of internal addresses may be allowed. The SDT's intent is that the Responsible Entity knows what other Cyber Assets or ranges of addresses a BES Cyber System needs to communicate with and limits the communications to that known range. For example, most BES Cyber Systems within a Responsible Entity should not have the ability to communicate through an EAP to any network address in the world, but should probably be at least limited to the address space of the Responsible Entity, and preferably to individual subnet ranges or individual hosts within the Responsible Entity's address space. The SDT's intent is not for Responsible Entities to document the inner workings of stateful firewalls, where connections initiated in one direction are allowed a return path. The intent is to know and document what systems can talk to what other systems or ranges of systems on the other side of the EAP, such that rogue connections can be detected and blocked.

This requirement applies only to communications for which access lists and 'deny by default' type requirements can be universally applied, which today are those that employ routable protocols. Direct serial, non-routable connections are not included as there is no perimeter or firewall type security that should be universally mandated across all entities and all serial communication situations. There is no firewall or perimeter capability for an RS232 cable run

between two Cyber Assets. Without a clear 'perimeter type' security control that can be applied in practically every circumstance, such a requirement would mostly generate technical feasibility exceptions ("TFEs") rather than increased security.

As for dial-up connectivity, the Standard Drafting Team's intent of this requirement is to prevent situations where only a phone number can establish direct connectivity to the BES Cyber Asset. If a dial-up modem is implemented in such a way that it simply answers the phone and connects the line to the BES Cyber Asset with no authentication of the calling party, it is a vulnerability to the BES Cyber System. The requirement calls for some form of authentication of the calling party before completing the connection to the BES Cyber System. Some examples of acceptable methods include dial-back modems, modems that must be remotely enabled or powered up, and modems that are only powered on by onsite personnel when needed along with policy that states they are disabled after use. If the dial-up connectivity is used for Interactive Remote Access, then Requirement R2 also applies.

The standard adds a requirement to detect malicious communications for Control Centers. This is in response to FERC Order No. 706, Paragraphs 496-503, where ESPs are required to have two distinct security measures such that the BES Cyber Systems do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear that this is not simply redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs. Technologies meeting this requirement include Intrusion Detection or Intrusion Prevention Systems (IDS/IPS) or other forms of deep packet inspection. These technologies go beyond source/destination/port rule sets and thus provide another distinct security measure at the ESP.

Requirement R2:

See Secure Remote Access Reference Document (see remote access alert).

Rationale

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

Rationale for R1:
The Electronic Security Perimeter ("ESP") serves to control traffic at the external electronic boundary of the BES Cyber System. It provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

Summary of Changes: CIP-005, Requirement R1 has taken more of a focus on the discrete Electronic Access Points, rather than the logical "perimeter."

CIP-005 (V1 through V4), Requirement R1.2 has been deleted from V5. This requirement was definitional in nature and used to bring dial-up modems using non-routable protocols into the scope of CIP-005. The non-routable protocol exclusion no longer exists as a blanket CIP-002 filter for applicability in V5, therefore there is no need for this requirement.

CIP-005 (V1 through V4), Requirement R1.1 and R1.3 were also definitional in nature and have been deleted from V5 as separate requirements but the concepts were integrated into the definitions of ESP and Electronic Access Point ("EAP").

Reference to prior version: (Part 1.1) CIP-005-4, R1

Change Rationale: (Part 1.1)
Explicitly clarifies that BES Cyber Assets connected via routable protocol must be in an Electronic Security Perimeter.

Reference to prior version: (Part 1.2) CIP-005-4, R1

Change Rationale: (Part 1.2)
Changed to refer to the defined term Electronic Access Point and BES Cyber System.

Reference to prior version: (Part 1.3) CIP-005-4, R2.1

Change Rationale: (Part 1.3)
Changed to refer to the defined term Electronic Access Point and to focus on the entity knowing and having a reason for what it allows through the EAP in both inbound and outbound directions.

Reference to prior version: (Part 1.4) CIP-005-4, R2.3

Change Rationale: (Part 1.4)
Added clarification that dial-up connectivity should perform authentication so that the BES Cyber System is not directly accessible with a phone number only.

Reference to prior version: (Part 1.5) CIP-005-4, R1

Change Rationale: (Part 1.5)
Per FERC Order No. 706, Paragraphs 496-503, ESPs need two distinct security measures such that the Cyber Assets do not lose all perimeter protection if one measure fails or is misconfigured. The Order makes clear this is not simple redundancy of firewalls, thus the SDT has decided to add the security measure of malicious traffic inspection as a requirement for these ESPs.

Rationale for R2:
Registered Entities use Interactive Remote Access to access Cyber Assets to support and maintain control systems networks. Discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of electric sector entities, necessitate changes to industry security control standards. Currently, no requirements are in effect for management of secure remote access to Cyber Assets to be afforded the NERC CIP protective measures. Inadequate safeguards for remote access can allow unauthorized access to the organization's network, with potentially serious consequences. Additional information is provided in ***Guidance for Secure Interactive Remote Access*** published by NERC in July 2011.

Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques. Remote access to the organization's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

The Intermediate System serves as a proxy for the remote user. Rather than allowing all the protocols the user might need to access Cyber Assets inside the Electronic Security Perimeter to traverse from the Electronic Security Perimeter to the remote computer, only the protocol required for remotely controlling the jump host is required. This allows the firewall rules to be much more restrictive than if the remote computer was allowed to connect to Cyber Assets within the Electronic Security Perimeter directly. The use of an Intermediate System also protects the Cyber Asset from vulnerabilities on the remote computer.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factor(s) used for authentication are acquired along with it.

Encryption is used to protect the data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. This is especially important when using the Internet as the communication means.

Summary of Changes: This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.1) New

Change Rationale: (Part 2.1)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3.

Reference to prior version: (Part 2.2) CIP-007-5, R3.1

Change Rationale: (Part 2.2)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The purpose of this part is to protect the confidentiality and integrity of each Interactive Remote Access session.

Reference to prior version: (Part 2.3) CIP-007-5, R3.2

Change Rationale: (Part 2.3)
This is a new requirement to continue the efforts of the Urgent Action team for Project 2010-15: Expedited Revisions to CIP-005-3. The multi-factor authentication methods are also the same as those identified in the Homeland Security Presidential Directive 12 (HSPD-12), issued August 12, 2007.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	May 2 – June 15, 2017

Anticipated Actions	Date
10-day final ballot	July 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

Rationale for Requirement R1:
Proposed requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The 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.

Guidance and examples are provided in the Guidelines and Technical Basis Section of this standard.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	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.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets

and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

CIP-010-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

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

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This 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. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

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

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard is adopted by the NERC Board of Trustees (Board).

Description of Current Draft

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	May 2 – June 15, 2017

Anticipated Actions	Date
10-day final ballot	July 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s):

None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-010-3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Interchange Coordinator or Interchange Authority

4.1.6. Reliability Coordinator

4.1.7. Transmission Operator

4.1.8. Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-010-3:

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

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

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

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

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

5. Effective Date:

See Implementation Plan for Project 2016-03.

6. Background: Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

Similarly, the term *program* may refer to the organization's overall implementation of its policies, plans, and procedures involving a subject matter. Examples in the

standards include the personnel risk assessment program and the personnel training program. The full implementation of the CIP Cyber Security Standards could also be referred to as a program. However, the terms *program* and *plan* do not imply any additional requirements beyond what is stated in the standards.

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

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

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples

may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.

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

B. Requirements and Measures

Rationale for Requirement R1:
Proposed requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The 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.

Guidance and examples are provided in the Guidelines and Technical Basis Section of this standard.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-010-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	~~For~~ 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.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed ~~during~~ prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-010-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-010-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets

and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority: "Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention: The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full-time period since the last audit.

The applicable entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

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

1.3. Compliance Monitoring and Enforcement Program: As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3) OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2.	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days. (2.1)
R3.	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has	The Responsible Entity has not implemented any vulnerability assessment processes for one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 18 months, but since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
				assessments, the action plans to remediate or mitigate vulnerabilities identified in the assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4.	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document the Removable Media sections	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media plan, but failed to document mitigation of software	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-3, Requirement R4. (R4)

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
	according to CIP-010-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Section 1.2. (R4)	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-3, Requirement R4,	

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
		Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Associated Documents

None.

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact

Version	Date	Action	Change Tracking
			BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-3. Docket No. RM15-14-000	
3	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

CIP-010-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

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

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-010-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or

other custom software developed for a specific task or function for the entity's use. If additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification~~Integrity and Authenticity~~

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source~~and authenticity~~) is a key control in preventing the introduction of malware or counterfeit software. This 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. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches. ~~That is why the requirement was not placed in CIP-007 - Security Patch Management.~~

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and ~~that the integrity of information systems~~ verify the integrity of the software using controls such as digital signatures~~and obtaining software directly from the developer~~. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware ~~of~~ or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

~~It is not the intent of the SDT to require a verification of each source or software update at the time it is obtained. It is sufficient to establish the reliable source and software update once. This will allow automated solutions to be implemented to obtain frequent updates such as patches.~~

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support. Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the

BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale

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

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010 and CIP-007 to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

A. Introduction

1. **Title:** Cyber Security — Configuration Change Management and Vulnerability Assessments

2. **Number:** CIP-0~~10-2~~10-3

3. **Purpose:** To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

4. **Applicability:**

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

4.1.1 Balancing Authority

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

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

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

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

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

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

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

4.1.3 Generator Operator

4.1.4 Generator Owner

4.1.5 Interchange Coordinator or Interchange Authority

4.1.6 Reliability Coordinator

4.1.7 Transmission Operator

4.1.8 Transmission Owner

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

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

4.2.1.1 Each UFLS or UVLS System that:

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

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

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

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

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

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

All BES Facilities.

4.2.3 **Exemptions:** The following are exempt from Standard CIP-0~~10-2~~10-3:

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

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

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

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

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

5. Effective Dates:

See Implementation Plan for ~~CIP-010-2~~Project 2016-03.

6. Background:

Standard CIP-010 exists as part of a suite of CIP Standards related to cyber security, which require the initial identification and categorization of BES Cyber Systems and require a minimum level of organizational, operational and procedural controls to mitigate risk to BES Cyber Systems.

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

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

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

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

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

Measures for the initial requirement are simply the documented processes themselves. Measures in the table rows provide examples of evidence to show

documentation and implementation of applicable items in the documented processes. These measures serve to provide guidance to entities in acceptable records of compliance and should not be viewed as an all-inclusive list.

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

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

"Applicable Systems" Columns in Tables:

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

- **High Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as high impact according to the CIP-002-5.1 identification and categorization processes.
- **Medium Impact BES Cyber Systems** – Applies to BES Cyber Systems categorized as medium impact according to the CIP-002-5.1 identification and categorization processes.
- **Electronic Access Control or Monitoring Systems (EACMS)** – Applies to each Electronic Access Control or Monitoring System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System. Examples may include, but are not limited to, firewalls, authentication servers, and log monitoring and alerting systems.
- **Physical Access Control Systems (PACS)** – Applies to each Physical Access Control System associated with a referenced high impact BES Cyber System or medium impact BES Cyber System with External Routable Connectivity.
- **Protected Cyber Assets (PCA)** – Applies to each Protected Cyber Asset associated with a referenced high impact BES Cyber System or medium impact BES Cyber System.

B. Requirements and Measures

Rationale for Requirement R1:
Proposed requirement R1 Part 1.6 addresses directives in Order No. 829 for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The 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.

Guidance and examples are provided in the Guidelines and Technical Basis Section of this standard.

R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M1. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	Examples of evidence may include, but are not limited to: • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset, individually or by group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset, individually or by group.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Authorize and document changes that deviate from the existing baseline configuration.	Examples of evidence may include, but are not limited to: • A change request record and associated electronic authorization (performed by the individual or group with the authority to authorize the change) in a change management system for each change; or • Documentation that the change was performed in accordance with the requirement.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	An example of evidence may include, but is not limited to, updated baseline documentation with a date that is within 30 calendar days of the date of the completion of the change.
1.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification.	An example of evidence may include, but is not limited to, a list of cyber security controls verified or tested along with the dated test results.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.5	High Impact BES Cyber Systems	Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a list of cyber security controls tested along with successful test results and a list of differences between the production and test environments with descriptions of how any differences were accounted for, including of the date of the test.

CIP-0~~10-2~~10-3 Table R1 – Configuration Change Management			
Part	**Applicable Systems**	**Requirements**	**Measures**
1.6	High Impact BES Cyber Systems Medium Impact BES Cyber Systems Note: Implementation 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 Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	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.	An example of evidence may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R2 – Configuration Monitoring* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-0~~10-2~~10-3 Table R2 – Configuration Monitoring			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; and 2. PCA	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	An example of evidence may include, but is not limited to, logs from a system that is monitoring the configuration along with records of investigation for any unauthorized changes that were detected.

R3. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R3– Vulnerability Assessments*. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M3. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Examples of evidence may include, but are not limited to: • A document listing the date of the assessment (performed at least once every 15 calendar months), the controls assessed for each BES Cyber System along with the method of assessment; or • A document listing the date of the assessment and the output of any tools used to perform the assessment.

CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.2	High Impact BES Cyber Systems	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed at least once every 36 calendar months), the output of the tools used to perform the assessment, and a list of differences between the production and test environments with descriptions of how any differences were accounted for in conducting the assessment.

CIP-0~~10-2~~10-3 Table R3 – Vulnerability Assessments			
Part	**Applicable Systems**	**Requirements**	**Measures**
3.3	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PCA	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	An example of evidence may include, but is not limited to, a document listing the date of the assessment (performed prior to the commissioning of the new Cyber Asset) and the output of any tools used to perform the assessment.
3.4	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	An example of evidence may include, but is not limited to, a document listing the results or the review or assessment, a list of action items, documented proposed dates of completion for the action plan, and records of the status of the action items (such as minutes of a status meeting, updates in a work order system, or a spreadsheet tracking the action items).

R4. Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]*

M4. Evidence shall include each of the documented plan(s) for Transient Cyber Assets and Removable Media that collectively include each of the applicable sections in Attachment 1 and additional evidence to demonstrate implementation of plan(s) for Transient Cyber Assets and Removable Media. Additional examples of evidence per section are located in Attachment 2. If a Responsible Entity does not use Transient Cyber Asset(s) or Removable Media, examples of evidence include, but are not limited to, a statement, policy, or other document that states the Responsible Entity does not use Transient Cyber Asset(s) or Removable Media.

C. Compliance

1. Compliance Monitoring Process:

1.1. Compliance Enforcement Authority:

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

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Assessment Processes:

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Additional Compliance Information:

None

2. Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	**Operations Planning**	**Medium**	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
					integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	requires authorization and documentation of changes that deviate from the existing baseline configuration. (1.2) OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration.(1.3) OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						that could be impacted by a change(s) that deviates from the existing baseline configuration. (1.4.1) OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change. (1.4.2 & 1.4.3)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration. (1.5.1) OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and production environments. (1.5.2) OR

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)
R2	**Operations Planning**	**Medium**	N/A	N/A	N/A	The Responsible Entity has not documented or implemented a process(es) to monitor for, investigate, and document detected unauthorized changes to the baseline at least once every 35 calendar days~~.~~ (2.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R3	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 15 months, but less than 18 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 18 months, but less than 21, months since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable	The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 21 months, but less than 24 months, since the last assessment on one of its applicable BES Cyber Systems. (3.1) OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for	The Responsible Entity has not implemented any vulnerability assessment processes for one of its applicable BES Cyber Systems. (R3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has performed a vulnerability assessment more than 24 months since the last assessment on one of its applicable BES Cyber Systems. (3.1)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-0~~10-2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Applicable Systems, but has performed an active vulnerability assessment more than 36 months, but less than 39 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Systems, but has performed an active vulnerability assessment more than 39 months, but less than 42 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	Applicable Systems, but has performed an active vulnerability assessment more than 42 months, but less than 45 months, since the last active assessment on one of its applicable BES Cyber Systems. (3.2)	OR The Responsible Entity has implemented one or more documented active vulnerability assessment processes for Applicable Systems, but has performed an active vulnerability assessment more than 45 months since the last active assessment on one of its applicable BES Cyber Systems.(3.2) OR The Responsible Entity has implemented and documented one or more vulnerability assessment processes for each of its applicable BES Cyber

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						Systems, but did not perform the active vulnerability assessment in a manner that models an existing baseline configuration of its applicable BES Cyber Systems. (3.3) OR The Responsible Entity has implemented one or more documented vulnerability assessment processes for each of its applicable BES Cyber Systems, but has not documented the results of the vulnerability assessments, the action plans to remediate or mitigate vulnerabilities identified in the

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
						assessments, the planned date of completion of the action plan, and the execution status of the mitigation plans. (3.4)
R4	**Long-term Planning and Operations Planning**	**Medium**	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to manage its Transient Cyber Asset(s) according to CIP-010-~~2~~10-3, Requirement R4, Attachment 1, Section 1.1. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to implement the Removable Media sections according to CIP-010-~~2~~10-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber	The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to authorize its Transient Cyber Asset(s) according to CIP-010-~~2~~10-3, Requirement R4, Attachment 1, Section 1.2. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber	The Responsible Entity failed to document or implement one or more plan(s) for Transient Cyber Assets and Removable Media according to CIP-010-~~2~~10-3, Requirement R4. (R4)

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2 10-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Assets and Removable Media, but failed to document the Removable Media sections according to CIP-010-2 10-3, Requirement R4, Attachment 1, Section 3. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media, but failed to document authorization for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2 10-3, Requirement R4,	Assets and Removable Media plan, but failed to document mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2 10-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and Removable Media,	Assets and Removable Media, but failed to implement mitigation of software vulnerabilities, mitigation for the introduction of malicious code, or mitigation of the risk of unauthorized use for Transient Cyber Assets managed by the Responsible Entity according to CIP-010-2 10-3, Requirement R4, Attachment 1, Sections 1.3, 1.4, and 1.5. (R4) OR The Responsible Entity documented its plan(s) for Transient Cyber Assets and	

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-~~2~~1-3)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
			Attachment 1, Section 1.2. (R4)	but failed to document mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~2~~1-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	Removable Media, but failed to implement mitigation of software vulnerabilities or mitigation for the introduction of malicious code for Transient Cyber Assets managed by a party other than the Responsible Entity according to CIP-010-~~2~~1-3, Requirement R4, Attachment 1, Sections 2.1, 2.2, and 2.3. (R4)	

D. Regional Variances

None.

E. Interpretations

None.

F. Associated Documents

Guideline and Technical Basis (attached).

Version History

Version	Date	Action	Change Tracking
1	11/26/12	Adopted by the NERC Board of Trustees.	Developed to define the configuration change management and vulnerability assessment requirements in coordination with other CIP standards and to address the balance of the FERC directives in its Order 706.
1	11/22/13	FERC Order issued approving CIP-010-1. (Order becomes effective on 2/3/14.)	
2	11/13/14	Adopted by the NERC Board of Trustees.	Addressed two FERC directives from Order No. 791 related to identify, assess, and correct language and communication networks.
2	2/12/15	Adopted by the NERC Board of Trustees.	Replaces the version adopted by the Board on 11/13/2014. Revised version addresses remaining directives from Order No. 791 related to transient devices and low impact BES Cyber Systems.
2	1/21/16	FERC Order issued approving CIP-010-2. Docket No. RM15-14-000	

3	tbd	Modified to address certain directives in FERC Order No. 829.	Revised

CIP-0~~10-2~~10-3 - Attachment 1

Required Sections for Plans for Transient Cyber Assets and Removable Media

Responsible Entities shall include each of the sections provided below in their plan(s) for Transient Cyber Assets and Removable Media as required under Requirement R4.

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

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

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

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

1.2.2. Locations, either individually or by group; and

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

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

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

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

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

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

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

Section 2. Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity.

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

- Review of installed security patch(es);
- Review of security patching process used by the party;
- Review of other vulnerability mitigation performed by the party; or
- Other method(s) to mitigate software vulnerabilities.

2.2 Introduction of malicious code mitigation: Use one or a combination of the following methods to achieve the objective of mitigating malicious code (per Transient Cyber Asset capability):

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

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

Section 3. Removable Media

3.1. Removable Media Authorization: For each individual or group of Removable Media, each Responsible Entity shall authorize:

3.1.1. Users, either individually or by group or role; and

3.1.2. Locations, either individually or by group.

3.2. Malicious Code Mitigation: To achieve the objective of mitigating the threat of introducing malicious code to high impact or medium impact BES Cyber Systems and their associated Protected Cyber Assets, each Responsible Entity shall:

3.2.1. Use method(s) to detect malicious code on Removable Media using a Cyber Asset other than a BES Cyber System or Protected Cyber Assets; and

3.2.2. Mitigate the threat of detected malicious code on Removable Media prior to connecting the Removable Media to a high impact or medium impact BES Cyber System or associated Protected Cyber Assets.

CIP-0~~10-2~~10-3 - Attachment 2

Examples of Evidence for Plans for Transient Cyber Assets and Removable Media

Section 1.1: Examples of evidence for Section 1.1 may include, but are not limited to, the method(s) of management for the Transient Cyber Asset(s). This can be included as part of the Transient Cyber Asset plan(s), part of the documentation related to authorization of Transient Cyber Asset(s) managed by the Responsible Entity or part of a security policy.

Section 1.2: Examples of evidence for Section 1.2 may include, but are not limited to, documentation from asset management systems, human resource management systems, or forms or spreadsheets that show authorization of Transient Cyber Asset(s) managed by the Responsible Entity. Alternatively, this can be documented in the overarching plan document.

Section 1.3: Examples of evidence for Section 1.3 may include, but are not limited to, documentation of the method(s) used to mitigate software vulnerabilities posed by unpatched software such as security patch management implementation, the use of live operating systems from read-only media, system hardening practices or other method(s) to mitigate the software vulnerability posed by unpatched software. Evidence can be from change management systems, automated patch management solutions, procedures or processes associated with using live operating systems, or procedures or processes associated with system hardening practices. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.4: Examples of evidence for Section 1.4 may include, but are not limited to, documentation of the method(s) used to mitigate the introduction of malicious code such as antivirus software and processes for managing signature or pattern updates, application whitelisting practices, processes to restrict communication, or other method(s) to mitigate the introduction of malicious code. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the vendor or Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 1.5: Examples of evidence for Section 1.5 may include, but are not limited to, documentation through policies or procedures of the method(s) to restrict physical access; method(s) of the full-disk encryption solution along with the authentication protocol; method(s) of the multi-factor authentication solution; or documentation of other method(s) to mitigate the risk of unauthorized use.

Section 2.1: Examples of evidence for Section 2.1 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of installed security patch(es); memoranda, electronic mail, policies or contracts from parties other than the Responsible Entity that identify the security patching process or vulnerability mitigation performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail, system documentation or contracts that identifies acceptance by the Responsible Entity that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate software vulnerabilities for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the risk from unpatched software, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.2: Examples of evidence for Section 2.2 may include, but are not limited to, documentation from change management systems, electronic mail or procedures that document a review of the installed antivirus update level; memoranda, electronic mail, system documentation, policies or contracts from the party other than the Responsible Entity that identify the antivirus update process, the use of application whitelisting, use of live of operating systems or system hardening performed by the party other than the Responsible Entity; evidence from change management systems, electronic mail or contracts that identifies the Responsible Entity's acceptance that the practices of the party other than the Responsible Entity are acceptable; or documentation of other method(s) to mitigate malicious code for Transient Cyber Asset(s) managed by a party other than the Responsible Entity. If a Transient Cyber Asset does not have the capability to use method(s) that mitigate the introduction of malicious code, evidence may include documentation by the Responsible Entity or the party other than the Responsible Entity that identifies that the Transient Cyber Asset does not have the capability.

Section 2.3: Examples of evidence for Section 2.3 may include, but are not limited to, documentation from change management systems, electronic mail, or contracts that identifies a review to determine whether additional mitigations are necessary and that they have been implemented prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity.

Section 3.1: Examples of evidence for Section 3.1 may include, but are not limited to, documentation from asset management systems, human resource management systems, forms or spreadsheets that shows authorization of Removable Media. The documentation must identify Removable Media, individually or by group of Removable Media, along with the authorized users,

either individually or by group or role, and the authorized locations, either individually or by group.

Section 3.2: Examples of evidence for Section 3.2 may include, but are not limited to, documented process(es) of the method(s) used to mitigate malicious code such as results of scan settings for Removable Media, or implementation of on-demand scanning. Documented process(es) for the method(s) used for mitigating the threat of detected malicious code on Removable Media, such as logs from the method(s) used to detect malicious code that show the results of scanning and that show mitigation of detected malicious code on Removable Media or documented confirmation by the entity that the Removable Media was deemed to be free of malicious code.

Guidelines and Technical Basis

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

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

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

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

Requirement R1:

Baseline Configuration

The concept of establishing a Cyber Asset's baseline configuration is meant to provide clarity on requirement language found in previous CIP standard versions. Modification of any item within an applicable Cyber Asset's baseline configuration provides the triggering mechanism for when entities must apply change management processes.

Baseline configurations in CIP-010 consist of five different items: Operating system/firmware, commercially available software or open-source application software, custom software, logical network accessible port identification, and security patches. Operating system information identifies the software and version that is in use on the Cyber Asset. In cases where an independent operating system does not exist (such as for a protective relay), then firmware information should be identified. Commercially available or open-source application software identifies applications that were intentionally installed on the cyber asset. The use of the term "intentional" was meant to ensure that only software applications that were determined to be necessary for Cyber Asset use should be included in the baseline configuration. The SDT does not intend for notepad, calculator, DLL, device drivers, or other applications included in an operating system package as commercially available or open-source application software to be included. Custom software installed may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use. If

additional software was intentionally installed and is not commercially available or open-source, then this software could be considered custom software. If a specific device needs to communicate with another device outside the network, communications need to be limited to only the devices that need to communicate per the requirement in CIP-007-6. Those ports which are accessible need to be included in the baseline. Security patches applied would include all historical and current patches that have been applied on the cyber asset. While CIP-007-6 Requirement R2, Part 2.1 requires entities to track, evaluate, and install security patches, CIP-010 Requirement R1, Part 1.1.5 requires entities to list all applied historical and current patches.

Further guidance can be understood with the following example that details the baseline configuration for a serial-only microprocessor relay:

Asset #051028 at Substation Alpha

- R1.1.1 – Firmware: [MANUFACTURER]-[MODEL]-XYZ-1234567890-ABC
- R1.1.2 – Not Applicable
- R1.1.3 – Not Applicable
- R1.1.4 – Not Applicable
- R1.1.5 – Patch 12345, Patch 67890, Patch 34567, Patch 437823

Also, for a typical IT system, the baseline configuration could reference an IT standard that includes configuration details. An entity would be expected to provide that IT standard as part of their compliance evidence.

Cyber Security Controls

The use of cyber security controls refers specifically to controls referenced and applied according to CIP-005 and CIP-007. The concept presented in the relevant requirement sub-parts in CIP-010 R1 is that an entity is to identify/verify controls from CIP-005 and CIP-007 that could be impacted for a change that deviates from the existing baseline configuration. The SDT does not intend for Responsible Entities to identify/verify all controls located within CIP-005 and CIP-007 for each change. The Responsible Entity is only to identify/verify those control(s) that could be affected by the baseline configuration change. For example, changes that affect logical network ports would only involve CIP-007 R1 (Ports and Services), while changes that affect security patches would only involve CIP-007 R2 (Security Patch Management). The SDT chose not to identify the specific requirements from CIP-005 and CIP-007 in CIP-010 language as the intent of the related requirements is to be able to identify/verify any of the controls in those standards that are affected as a result of a change to the baseline configuration. The SDT believes it possible that all requirements from CIP-005 and CIP-007 may be identified for a

major change to the baseline configuration, and therefore, CIP-005 and CIP-007 was cited at the standard-level versus the requirement-level.

Test Environment

The Control Center test environment (or production environment where the test is performed in a manner that minimizes adverse effects) should model the baseline configuration, but may have a different set of components. For instance, an entity may have a BES Cyber System that runs a database on one component and a web server on another component. The test environment may have the same operating system, security patches, network accessible ports, and software, but have both the database and web server running on a single component instead of multiple components.

Additionally, the Responsible Entity should note that wherever a test environment (or production environment where the test is performed in a manner that minimizes adverse effects) is mentioned, the requirement is to "model" the baseline configuration and not duplicate it exactly. This language was chosen deliberately in order to allow for individual elements of a BES Cyber System at a Control Center to be modeled that may not otherwise be able to be replicated or duplicated exactly; such as, but not limited to, a legacy map-board controller or the numerous data communication links from the field or to other Control Centers (such as by ICCP).

Software Verification

The concept of software verification (verifying the identity of the software source and the integrity of the software obtained from the software source) is a key control in preventing the introduction of malware or counterfeit software. This 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. The intent of the SDT is for Responsible Entities to provide controls for verifying the baseline elements that are updated by vendors. It is important to note that this is not limited to only security patches.

NIST SP-800-161 includes a number of security controls, which, when taken together, reduce the probability of a successful "Watering Hole" or similar cyber attack in the industrial control system environment and thus could assist in addressing this objective. For example, in the System and Information Integrity (SI) control family, control SI-7 suggests users obtain software directly from the developer and verify the integrity of the software using controls such as digital signatures. In the Configuration Management (CM) control family, control CM-5(3) requires that the information system prevent the installation of firmware or software without the verification that the component has been digitally signed to ensure that the hardware and software components are genuine and valid. NIST SP-800-161, while not meant to be definitive, provides examples of controls for addressing this objective. Other controls also could meet this objective.

In implementing Requirement R1 Part 1.6, the responsible entity should consider their existing CIP cyber security policies and controls in addition to the following:

- Processes used to deliver software and appropriate control(s) that will verify the identity of the software source and the integrity of the software delivered through these processes. To the extent that the responsible entity utilizes automated systems such as a subscription service to download and distribute software including updates, consider how software verification can be performed through those processes.
- Coordination of the responsible entity's software verification control(s) with other cyber security policies and controls, including change management and patching processes, and procurement controls.
- Use of a secure central software repository after the identity of the software source and the integrity of the software have been validated, so that verifications do not need to be performed repeatedly before each installation.
- Additional controls such as examples outlined in the Software, Firmware, and Information Integrity (SI-7) section of NIST Special Publication 800-53 Revision 4, or similar guidance.
- Additional controls such as those defined in FIPS-140-2, FIPS 180-4, or similar guidance, to ensure the cryptographic methods used are acceptable to the Responsible Entity.

Responsible entities may use various methods to verify the integrity of software obtained from the software source. Examples include, but are not limited to, the following:

- Verify that the software has been digitally signed and validate the signature to ensure that the software's integrity has not been compromised.
- Use public key infrastructure (PKI) with encryption to ensure that the software is not modified in transit by enabling only intended recipients to decrypt the software.
- Require software sources to provide fingerprints or cipher hashes for all software and verify the values prior to installation on a BES Cyber System to ensure the integrity of the software. Consider using a method for receiving the verification values that is different from the method used to receive the software from the software source.
- Use trusted/controlled distribution and delivery options to reduce supply chain risk (e.g., requiring tamper-evident packaging of software during shipping.)

Requirement R2:

The SDT's intent of R2 is to require automated monitoring of the BES Cyber System. However, the SDT understands that there may be some Cyber Assets where automated monitoring may not be possible (such as a GPS time clock). For that reason, automated technical monitoring was not explicitly required, and a Responsible Entity may choose to accomplish this requirement through manual procedural controls.

Requirement R3:

The Responsible Entity should note that the requirement provides a distinction between paper and active vulnerability assessments. The justification for this distinction is well-documented in FERC Order No. 706 and its associated Notice of Proposed Rulemaking. In developing their vulnerability assessment processes, Responsible Entities are strongly encouraged to include at least the following elements, several of which are referenced in CIP-005 and CIP-007:

Paper Vulnerability Assessment:

1. Network Discovery - A review of network connectivity to identify all Electronic Access Points to the Electronic Security Perimeter.
2. Network Port and Service Identification - A review to verify that all enabled ports and services have an appropriate business justification.
3. Vulnerability Review - A review of security rule-sets and configurations including controls for default accounts, passwords, and network management community strings.
4. Wireless Review - Identification of common types of wireless networks (such as 802.11a/b/g/n) and a review of their controls if they are in any way used for BES Cyber System communications.

Active Vulnerability Assessment:

1. Network Discovery - Use of active discovery tools to discover active devices and identify communication paths in order to verify that the discovered network architecture matches the documented architecture.
2. Network Port and Service Identification – Use of active discovery tools (such as Nmap) to discover open ports and services.
3. Vulnerability Scanning – Use of a vulnerability scanning tool to identify network accessible ports and services along with the identification of known vulnerabilities associated with services running on those ports.
4. Wireless Scanning – Use of a wireless scanning tool to discover wireless signals and networks in the physical perimeter of a BES Cyber System. Serves to identify unauthorized wireless devices within the range of the wireless scanning tool.

In addition, Responsible Entities are strongly encouraged to review NIST SP800-115 for additional guidance on how to conduct a vulnerability assessment.

Requirement R4:

Because most BES Cyber Assets and BES Cyber Systems are isolated from external public or untrusted networks, Transient Cyber Assets and Removable Media are a means for cyber-attack. Transient Cyber Assets and Removable Media are often the only way to transport files to and from secure areas to maintain, monitor, or troubleshoot critical systems. To protect the BES Cyber Assets and BES Cyber Systems, entities are required to document and implement a plan for how they will manage the use of Transient Cyber Assets and Removable Media. The

approach of defining a plan allows the Responsible Entity to document the processes that are supportable within its organization and in alignment with its change management processes.

Transient Cyber Assets and Removable Media are those devices connected temporarily to: (1) a BES Cyber Asset, (2) a network within an ESP, or (3) a Protected Cyber Asset. Transient Cyber Assets and Removable Media do not provide BES reliability services and are not part of the BES Cyber Asset to which they are connected. Examples of these temporarily connected devices include, but are not limited to:

- Diagnostic test equipment;
- Packet sniffers;
- Equipment used for BES Cyber System maintenance;
- Equipment used for BES Cyber System configuration; or
- Equipment used to perform vulnerability assessments.

Transient Cyber Assets can be one of many types of devices from a specially-designed device for maintaining equipment in support of the BES to a platform such as a laptop, desktop, or tablet that may just interface with or run applications that support BES Cyber Systems and is capable of transmitting executable code. Removable Media in scope of this requirement can be in the form of floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory.

While the definitions of Transient Cyber Asset and Removable Media include a conditional provision that requires them to be connected for 30 days or less, Section 1.1 of Attachment 1 allows the Responsible Entity to include provisions in its plan(s) that allow continuous or on-demand treatment and application of controls independent of the connected state. Please note that for on-demand treatment, the requirements only apply when Transient Cyber Assets and Removable Media are being connected to a BES Cyber System or Protected Cyber Asset. Once the transient device is disconnected, the requirements listed herein are not applicable until that Transient Cyber Asset or Removable Media is to be reconnected to the BES Cyber Asset or Protected Cyber Asset.

The attachment was created to specify the capabilities and possible security methods available to Responsible Entities based upon asset type, ownership, and management.

With the list of options provided in Attachment 1 for each control area, the entity has the discretion to use the option(s) that is most appropriate. This includes documenting its approach for how and when the entity manages or reviews the Transient Cyber Asset under its control or under the control of parties other than the Responsible Entity. The entity should avoid implementing a security function that jeopardizes reliability by taking actions that would negatively impact the performance or support of the Transient Cyber Asset, BES Cyber Asset, or Protected Cyber Asset.

Vulnerability Mitigation

The terms “mitigate”, “mitigating”, and “mitigation” are used in the sections in Attachment 1 to address the risks posed by malicious code, software vulnerabilities, and unauthorized use when

connecting Transient Cyber Assets and Removable Media. Mitigation in this context does not require that each vulnerability is individually addressed or remediated, as many may be unknown or not have an impact on the system to which the Transient Cyber Asset or Removable Media is connected. Mitigation is meant to reduce security risks presented by connecting the Transient Cyber Asset.

Per Transient Cyber Asset Capability

As with other CIP standards, the requirements are intended for an entity to use the method(s) that the system is capable of performing. The use of "per Transient Cyber Asset capability" is to eliminate the need for a Technical Feasibility Exception when it is understood that the device cannot use a method(s). For example, for malicious code, many types of appliances are not capable of implementing antivirus software; therefore, because it is not a capability of those types of devices, implementation of the antivirus software would not be required for those devices.

Requirement R4, Attachment 1, Section 1 - Transient Cyber Asset(s) Managed by the Responsible Entity

Section 1.1: Entities have a high level of control for the assets that they manage. The requirements listed herein allow entities the flexibility to either pre-authorize an inventory of devices or authorize devices at the time of connection or use a combination of these methods. The devices may be managed individually or by group.

Section 1.2: Entities are to document and implement their process(es) to authorize the use of Transient Cyber Assets for which they have direct management. The Transient Cyber Assets may be listed individually or by asset type. To meet this requirement part, the entity is to document the following:

1.2.1 User(s), individually or by group/role, allowed to use the Transient Cyber Asset(s). This can be done by listing a specific person, department, or job function. Caution: consider whether these user(s) must also have authorized electronic access to the applicable system in accordance with CIP-004.

1.2.2 Locations where the Transient Cyber Assets may be used. This can be done by listing a specific location or a group of locations.

1.2.3 The intended or approved use of each individual, type, or group of Transient Cyber Asset. This should also include the software or application packages that are authorized with the purpose of performing defined business functions or tasks (e.g., used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes), and approved network interfaces (e.g., wireless, including near field communication or Bluetooth, and wired connections). Activities, and software or application packages, not specifically listed as acceptable should be considered as prohibited. It may be beneficial to educate individuals through the CIP-004 Security Awareness Program and Cyber Security Training Program about authorized and unauthorized activities or uses (e.g.,

using the device to browse the Internet or to check email or using the device to access wireless networks in hotels or retail locations).

Entities should exercise caution when using Transient Cyber Assets and ensure they do not have features enabled (e.g., wireless or Bluetooth features) in a manner that would allow the device to bridge an outside network to an applicable system. Doing so would cause the Transient Cyber Asset to become an unauthorized Electronic Access Point in violation of CIP-005, Requirement R1.

Attention should be paid to Transient Cyber Assets that may be used for assets in differing impact areas (i.e., high impact, medium impact, and low impact). These impact areas have differing levels of protection under the CIP requirements, and measures should be taken to prevent the introduction of malicious code from a lower impact area. An entity may want to consider the need to have separate Transient Cyber Assets for each impact level.

Section 1.3: Entities are to document and implement their process(es) to mitigate software vulnerabilities posed by unpatched software through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. Recognizing there is a huge diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in software vulnerability management solutions, options are listed that include the alternative for the entity to use a technology or process that effectively mitigates vulnerabilities.

- Security patching, including manual or managed updates provides flexibility to the Responsible Entity to determine how its Transient Cyber Asset(s) will be used. It is possible for an entity to have its Transient Cyber Asset be part of an enterprise patch process and receive security patches on a regular schedule or the entity can verify and apply security patches prior to connecting the Transient Cyber Asset to an applicable Cyber Asset. Unlike CIP-007, Requirement R2, there is no expectation of creating dated mitigation plans or other documentation other than what is necessary to identify that the Transient Cyber Asset is receiving appropriate security patches.
- Live operating system and software executable only from read-only media is provided to allow a protected operating system that cannot be modified to deliver malicious software. When entities are creating custom live operating systems, they should check the image during the build to ensure that there is not malicious software on the image.
- System hardening, also called operating system hardening, helps minimize security vulnerabilities by removing all non-essential software programs and utilities and only installing the bare necessities that the computer needs to function. While other programs may provide useful features, they can provide "back-door" access to the system, and should be removed to harden the system.
- When selecting to use other methods that mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet the software vulnerability mitigation objective.

Section 1.4: Entities are to document and implement their process(es) to mitigate malicious code through the use of one or more of the protective measures listed. This needs to be applied based on the capability of the device. As with vulnerability management, there is diversity of the types of devices that can be included as Transient Cyber Assets and the advancement in malicious code protections. When addressing malicious code protection, the Responsible Entity should address methods deployed to deter, detect, or prevent malicious code. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident.

- Antivirus software, including manual or managed updates of signatures or patterns, provides flexibility just as with security patching, to manage Transient Cyber Asset(s) by deploying antivirus or endpoint security tools that maintain a scheduled update of the signatures or patterns. Also, for devices that do not regularly connect to receive scheduled updates, entities may choose to scan the Transient Cyber Asset prior to connection to ensure no malicious software is present.
- Application whitelisting is a method of authorizing only the applications and processes that are necessary on the Transient Cyber Asset. This reduces the opportunity that malicious software could become resident, much less propagate, from the Transient Cyber Asset to the BES Cyber Asset or BES Cyber System.
- Restricted communication to limit the exchange of data to only the Transient Cyber Asset and the Cyber Assets to which it is connected by restricting or disabling serial or network (including wireless) communications on a managed Transient Cyber Asset can be used to minimize the opportunity to introduce malicious code onto the Transient Cyber Asset while it is not connected to BES Cyber Systems. This renders the device unable to communicate with devices other than the one to which it is connected.
- When selecting to use other methods that mitigate the introduction of malicious code to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the introduction of malicious code objective.

Section 1.5: Entities are to document and implement their process(es) to protect and evaluate Transient Cyber Assets to ensure they mitigate the risks that unauthorized use of the Transient Cyber Asset may present to the BES Cyber System. The concern addressed by this section is the possibility that the Transient Cyber Asset could be tampered with, or exposed to malware, while not in active use by an authorized person. Physical security of the Transient Cyber Asset is certainly a control that will mitigate this risk, but other tools and techniques are also available. The bulleted list of example protections provides some suggested alternatives.

- For restricted physical access, the intent is that the Transient Cyber Asset is maintained within a Physical Security Perimeter or other physical location or enclosure that uses physical access controls to protect the Transient Cyber Asset.
- Full disk encryption with authentication is an option that can be employed to protect a Transient Cyber Asset from unauthorized use. However, it is important that

authentication be required to decrypt the device. For example, pre-boot authentication, or power-on authentication, provides a secure, tamper-proof environment external to the operating system as a trusted authentication layer. Authentication prevents data from being read from the hard disk until the user has confirmed they have the correct password or other credentials. By performing the authentication prior to the system decrypting and booting, the risk that an unauthorized person may manipulate the Transient Cyber Asset is mitigated.

- Multi-factor authentication is used to ensure the identity of the person accessing the device. Multi-factor authentication also mitigates the risk that an unauthorized person may manipulate the Transient Cyber Asset.
- In addition to authentication and pure physical security methods, other alternatives are available that an entity may choose to employ. Certain theft recovery solutions can be used to locate the Transient Cyber Asset, detect access, remotely wipe, and lockout the system, thereby mitigating the potential threat from unauthorized use if the Transient Cyber Asset was later connected to a BES Cyber Asset. Other low tech solutions may also be effective to mitigate the risk of using a maliciously-manipulated Transient Cyber Asset, such as tamper evident tags or seals, and executing procedural controls to verify the integrity of the tamper evident tag or seal prior to use.
- When selecting to use other methods that mitigate the risk of unauthorized use to those listed, entities need to have documentation that identifies how the other method(s) meet the mitigation of the risk of unauthorized use objective.

Requirement R4, Attachment 1, Section 2 - Transient Cyber Asset(s) Managed by a Party Other than the Responsible Entity

The attachment also recognizes the lack of control for Transient Cyber Assets that are managed by parties other than the Responsible Entity. However, this does not obviate the Responsible Entity's responsibility to ensure that methods have been deployed to deter, detect, or prevent malicious code on Transient Cyber Assets it does not manage. The requirements listed herein allow entities the ability to review the assets to the best of their capability and to meet their obligations.

To facilitate these controls, Responsible Entities may choose to execute agreements with other parties to provide support services to BES Cyber Systems and BES Cyber Assets that may involve the use of Transient Cyber Assets. Entities may consider using the Department of Energy Cybersecurity Procurement Language for Energy Delivery dated April 2014. [1] Procurement language may unify the other party and entity actions supporting the BES Cyber Systems and BES Cyber Assets. CIP program attributes may be considered including roles and responsibilities, access controls, monitoring, logging, vulnerability, and patch management along with incident response and back up recovery may be part of the other party's support.

[1] http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014

Entities should consider the "General Cybersecurity Procurement Language" and "The Supplier's Life Cycle Security Program" when drafting Master Service Agreements, Contracts, and the CIP program processes and controls.

Section 2.1: Entities are to document and implement their process(es) to mitigate software vulnerabilities through the use of one or more of the protective measures listed.

- Conduct a review of the Transient Cyber Asset managed by a party other than the Responsible Entity to determine whether the security patch level of the device is adequate to mitigate the risk of software vulnerabilities before connecting the Transient Cyber Asset to an applicable system.
- Conduct a review of the other party's security patching process. This can be done either at the time of contracting but no later than prior to connecting the Transient Cyber Asset to an applicable system. Just as with reviewing the security patch level of the device, selecting to use this approach aims to ensure that the Responsible Entity has mitigated the risk of software vulnerabilities to applicable systems.
- Conduct a review of other processes that the other party uses to mitigate the risk of software vulnerabilities. This can be reviewing system hardening, application whitelisting, virtual machines, etc.
- When selecting to use other methods to mitigate software vulnerabilities to those listed, entities need to have documentation that identifies how the other method(s) meet mitigation of the risk of software vulnerabilities.

Section 2.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed.

- Review the use of antivirus software and signature or pattern levels to ensure that the level is adequate to the Responsible Entity to mitigate the risk of malicious software being introduced to an applicable system.
- Review the antivirus or endpoint security processes of the other party to ensure that their processes are adequate to the Responsible Entity to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of application whitelisting used by the other party to mitigate the risk of introducing malicious software to an applicable system.
- Review the use of live operating systems or software executable only from read-only media to ensure that the media is free from malicious software itself. Entities should review the processes to build the read-only media as well as the media itself.
- Review system hardening practices used by the other party to ensure that unnecessary ports, services, applications, etc. have been disabled or removed. This will limit the chance of introducing malicious software to an applicable system.

Section 2.3: Determine whether additional mitigation actions are necessary, and implement such actions prior to connecting the Transient Cyber Asset managed by a party other than the Responsible Entity. The intent of this section is to ensure that after conducting the selected review from Sections 2.1 and 2.2, if there are deficiencies that do not meet the Responsible Entity's security posture, the other party is required to complete the mitigations prior to connecting their devices to an applicable system.

Requirement R4, Attachment 1, Section 3 - Removable Media

Entities have a high level of control for Removable Media that are going to be connected to their BES Cyber Assets.

Section 3.1: Entities are to document and implement their process(es) to authorize the use of Removable Media. The Removable Media may be listed individually or by type.

- Document the user(s), individually or by group/role, allowed to use the Removable Media. This can be done by listing a specific person, department, or job function. Authorization includes vendors and the entity's personnel. Caution: consider whether these user(s) must have authorized electronic access to the applicable system in accordance with CIP-004.
- Locations where the Removable Media may be used. This can be done by listing a specific location or a group/role of locations.

Section 3.2: Entities are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more method(s) to detect malicious code on the Removable Media before it is connected to a BES Cyber Asset. When using the method(s) to detect malicious code, it is expected to occur from a system that is not part of the BES Cyber System to reduce the risk of propagating malicious code into the BES Cyber System network or onto one of the BES Cyber Assets. If malicious code is discovered, it must be removed or mitigated to prevent it from being introduced into the BES Cyber Asset or BES Cyber System. Entities should also consider whether the detected malicious code is a Cyber Security Incident. Frequency and timing of the methods used to detect malicious code were intentionally excluded from the requirement because there are multiple timing scenarios that can be incorporated into a plan to mitigate the risk of malicious code. The entities must use the method(s) to detect malicious code on Removable Media before it is connected to the BES Cyber Asset. The timing dictated and documented in the entity's plan should reduce the risk of introducing malicious code to the BES Cyber Asset or Protected Cyber Asset.

As a method to detect malicious code, entities may choose to use Removable Media with on-board malicious code detection tools. For these tools, the Removable Media are still used in conjunction with a Cyber Asset to perform the detection. For Section 3.2.1, the Cyber Asset used to perform the malicious code detection must be outside of the BES Cyber System or Protected Cyber Asset.

Rationale:

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

Rationale for Requirement R1:
The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R2:
The configuration monitoring processes are intended to detect unauthorized modifications to BES Cyber Systems.

Rationale for Requirement R3:
The vulnerability assessment processes are intended to act as a component in an overall program to periodically ensure the proper implementation of cyber security controls as well as to continually improve the security posture of BES Cyber Systems.
The vulnerability assessment performed for this requirement may be a component of deficiency identification, assessment, and correction.

Rationale for R4:
Requirement R4 responds to the directive in FERC Order No. 791, at Paragraphs 6 and 136, to address security-related issues associated with Transient Cyber Assets and Removable Media used on a temporary basis for tasks such as data transfer, vulnerability assessment, maintenance, or troubleshooting. These tools are potential vehicles for transporting malicious code into a facility and subsequently into Cyber Assets or BES Cyber Systems. To mitigate the risks associated with such tools, Requirement R4 was developed to accomplish the following security objectives:

- Preventing unauthorized access or malware propagation to BES Cyber Systems through Transient Cyber Assets or Removable Media; and
- Preventing unauthorized access to BES Cyber System Information through Transient Cyber Assets or Removable Media.

Requirement R4 incorporates the concepts from other CIP requirements in CIP-010~~-2~~ and CIP-007~~-6~~ to help define the requirements for Transient Cyber Assets and Removable Media.

Summary of Changes: All requirements related to Transient Cyber Assets and Removable Media are included within a single standard, CIP-010. Due to the newness of the requirements and definition of asset types, the SDT determined that placing the requirements in a single standard would help ensure that entities were able to quickly identify the requirements for these asset types. A separate standard was considered for these requirements. However, the SDT determined that these types of assets would be used in relation to change management and vulnerability assessment processes and should, therefore, be placed in the same standard as those processes.

Standard Development Timeline

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

Description of Current Draft

This is the first draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	January 19 - March 6, 2017
45-day formal comment period with ballot	May 2 – June 15, 2017

Anticipated Actions	Date
10-day final ballot	July 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

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

   4.1.1. Balancing Authority

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

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

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

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

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

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

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

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

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

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

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

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

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

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

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

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

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

Rationale for Requirement R1:
The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES 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); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For

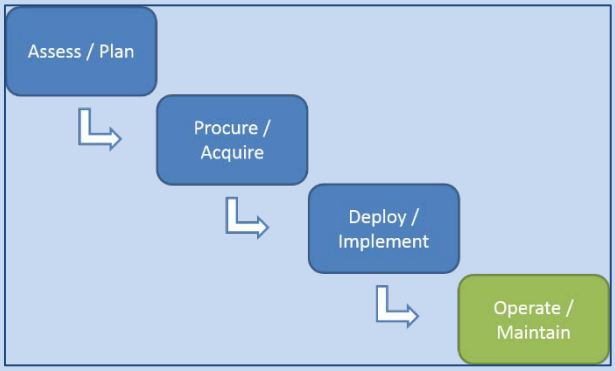
example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



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;

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).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

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.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited

to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

Rationale for Requirement R3:
The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

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. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

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

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

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

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within

	so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 829.	NA

Standard Attachments

None

Guidelines and Technical Basis

Rationale

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

Standard Development Timeline

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

Description of Current Draft

This is the first draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	January 19 - March 6, 2017
45-day formal comment period with ballot	May 2 – June 15, 2017

Anticipated Actions	Date
10-day final ballot	July 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

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

4.1.1. Balancing Authority

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

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

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

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

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

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

4.1.3. Generator Operator

4.1.4. Generator Owner

4.1.5. Reliability Coordinator

4.1.6. Transmission Operator

4.1.7. Transmission Owner

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

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

4.2.1.1. Each UFLS or UVLS System that:

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

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

Rationale for Requirement R1:
The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES 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); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of ~~elements contained in~~ the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation

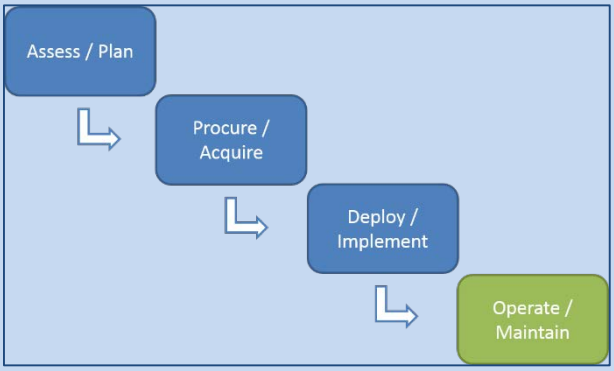
processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), ~~and in~~ negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



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;

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).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

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.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

Rationale for Requirement R3:
The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

- Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

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. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the ~~elements~~ parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the ~~elements~~ parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2.	~~N/A~~ The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~N/A~~ The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~N/A~~ The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within

	so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	TBD	Respond to FERC Order No. 829.	NA

Standard Attachments

None

Guidelines and Technical Basis

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT adoption, the text from the rationale text boxes was moved to this section.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard

Applicable Standard(s)

CIP-005-6 — Cyber Security — Electronic Security Perimeters

CIP-010-3 — Configuration Change Management and Vulnerability Assessments

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

CIP-005-5 — Cyber Security — Electronic Security Perimeters

CIP-010-2 — Configuration Change Management and Vulnerability Assessments

Prerequisite Standard(s)

None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
  - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator

- Transmission Operator
- Transmission Owner

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 apply only to BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing 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 Bulk Electric System (BES) operations. Order No. 829 (at P 2) states:

> [The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

FERC directed NERC to submit the new or modified Reliability Standard(s) within one year of the effective date of Order No. 829, i.e., by September 27, 2017.

General Considerations

Consistent with the directive to develop a forward-looking Reliability Standard, the implementation of Reliability Standards in Project 2016-03 do not require the abrogation or re-negotiation of contracts (including amendments to master agreements and purchase orders) with vendors, suppliers or other entities executed as of the effective date of the proposed Reliability Standards (See FERC Order No. 829, P. 36).

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-1.

Effective Date

For all Reliability Standards in Project 2016-03 — CIP-005-6, CIP-010-3, and CIP-013-1

Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

CIP-013-1 Requirement R3
The initial review and approval of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement R3 must be completed on or before the effective date of CIP-013-1.

Planned or Unplanned Changes Resulting in a Higher Categorizaton

Compliance timelines with CIP-005-6, CIP-010-3, and CIP-013-1 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards.

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5 (or any subsequent version of that Reliability Standard) which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For planned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 on the update of the identification and categorization of the affected BES Cyber System.

For unplanned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 according to the following timelines, following the identification and categorization of the affected BES Cyber System.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 Months
New medium impact BES Cyber System	12 Months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 Months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 Months

Retirement Date

Standards listed in the **Requested Retirement(s)** section shall be retired immediately prior to the effective date in the particular jurisdiction in which the revised standards are becoming effective.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation Plan

Project 2016-03 Cyber Security Supply Chain Risk Management Reliability Standard ~~CIP-013-1~~

Applicable Standard(s)

CIP-005-6 — Cyber Security — Electronic Security Perimeters

CIP-010-3 — Configuration Change Management and Vulnerability Assessments

CIP-013-1 — Cyber Security — Supply Chain Risk Management

Requested Retirement(s)

CIP-005-5 — Cyber Security — Electronic Security Perimeters

CIP-010-2 — Configuration Change Management and Vulnerability Assessments

Prerequisite Standard(s)

None

Applicable Entities

- Balancing Authority
- Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:
  - Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:
  - Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and
  - Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.
  - Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.
  - Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.
- Generator Operator
- Generator Owner
- Reliability Coordinator

- Transmission Operator
- Transmission Owner

Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 apply only to BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

Background

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing 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 Bulk Electric System (BES) operations. Order No. 829 (at P 2) states:

> [The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

FERC directed NERC to submit the new or modified Reliability Standard(s) within one year of the effective date of Order No. 829, i.e., by September 27, 2017.

General Considerations

Consistent with the directive to develop a forward-looking Reliability Standard, the implementation of Reliability Standards in Project 2016-03 do not require the abrogation or re-negotiation of contracts (including amendments to master agreements and purchase orders) with vendors, suppliers or other entities executed as of the effective date of the proposed Reliability Standards (See FERC Order No. 829, P. 36).

In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, ~~or~~ requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. ~~Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1.~~ Contract effective date, commencement date, or other activation dates specified in ~~the~~ a contract do not determine whether the ~~contract is~~procurement action is within scope of CIP-013-1.

Effective Date

For all Reliability Standards in Project 2016-03 — CIP-005-6, CIP-010-3, and CIP-013-1
Where approval by an applicable governmental authority is required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the effective date of the applicable governmental authority's order approving the Reliability Standard, or as otherwise provided for by the applicable governmental authority.

Where approval by an applicable governmental authority is not required, the Reliability Standard shall become effective on the first day of the first calendar quarter that is 18 months after the date the Reliability Standard is adopted by the NERC Board of Trustees, or as otherwise provided for in that jurisdiction.

Initial Performance of Periodic Requirements

CIP-013-1 Requirement R3
The initial review and approval of supply chain cyber security risk management plans by CIP Senior Manager or Delegate pursuant to Requirement R3 must be completed on or before the effective date of CIP-013-1.

Planned or Unplanned Changes Resulting in a Higher Categorizaton

Compliance timelines with CIP-005-6, CIP-010-3, and CIP-013-1 for planned or unplanned changes in categorization are consistent with the Implementation Plan associated with Project 2008-06 Cyber Security Order 706 Version 5 CIP Standards.

Planned changes refer to any changes of the electric system or BES Cyber System as identified through the annual assessment under CIP-002-5 (or any subsequent version of that Reliability Standard) which were planned and implemented by the responsible entity.

For example, if an automation modernization activity is performed at a transmission substation, whereby Cyber Assets are installed that meet the criteria in CIP-002-5, Attachment 1, then the new BES Cyber System has been implemented as a result of a planned change.

In contrast, *unplanned* changes refer to any changes of the electric system or BES Cyber System, as identified through the annual assessment under CIP-002-5, Requirement R2, which were not planned by the responsible entity. Consider the scenario where a particular BES Cyber System at a transmission substation does not meet the criteria in CIP-002-5, Attachment 1, then, later, an action is performed outside of that particular transmission substation; such as, a transmission line is constructed or retired, a generation plant is modified, changing its rated output, and that unchanged BES Cyber System may become a medium impact BES Cyber System based on the CIP-002-5, Attachment 1, criteria.

For planned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 on the update of the identification and categorization of the affected BES Cyber System.

For unplanned changes resulting in a higher categorization, the responsible entity shall comply with all applicable requirements in CIP-005-6, CIP-010-3, and CIP-013-1 according to the following timelines, following the identification and categorization of the affected BES Cyber System.

Scenario of Unplanned Changes After the Effective Date	Compliance Implementation
New high impact BES Cyber System	12 Months
New medium impact BES Cyber System	12 Months
Newly categorized high impact BES Cyber System from medium impact BES Cyber System	12 months for requirements not applicable to Medium-Impact BES Cyber Systems
Newly categorized medium impact BES Cyber System	12 Months
Responsible entity identifies first medium impact or high impact BES Cyber System (i.e., the responsible entity previously had no BES Cyber Systems categorized as high impact or medium impact according to the CIP-002-5 identification and categorization processes)	24 Months

~~**Definition**~~

~~None~~

Retirement Date

Standards listed in the **Requested Retirement(s)** section shall be retired immediately prior to the effective date in the particular jurisdiction in which the revised standards are becoming effective.

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-03 — Cyber Security — Supply Chain Risk Management

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **Project 2016-03 — Cyber Security — Supply Chain Risk Management.** Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines. The Cyber Security Supply Chain Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.
Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in an Operations Planning time horizon to develop one or more documented supply chain cyber security risk management plan(s). If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective, which is to develop one or more documented supply chain cyber security risk management plan(s). Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-013-1, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to develop one or more documented supply chain cyber security risk management plan(s) that set forth the controls.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in Operations Planning time horizon that requires entities to implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. If violated, failing to implement this plan could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) as specified in the requirement.

VSL Justifications for CIP-013-1, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R2 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSL is based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	R3 is a requirement in Operations Planning time horizon that requires the Responsible Entity to periodically review and obtain CIP Senior Manager or delegate approval of supply chain cyber security risk management plans. The reliability objective is to ensure plans remain up to date and address current and emerging supply chain-related cyber security concerns and vulnerabilities. If the requirement is violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R3 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of the review requirement by some number of months less than 18 calendar months does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-005-6, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in an Operations Planning and Same Day Operations time horizon to implement one or more documented processes for controlling vendor remote access to high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with the addition of two parts addressing specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-005-6, R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5)..	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

VSL Justifications for CIP-005-6, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	Theaddition of Parts 2.4 and 2.5 does not lower the current level of compliance.

the Current Level of Compliance	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R2 is not binary. Guideline 2b: The proposed VSLs do not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.

FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in Operations Planning time horizon that requires the Responsible Entity to implement one or more documented processes that include each of the applicable requirement parts for configuration change management. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with an additional part to address specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation

VSLs for CIP-010-3, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the	The Responsible Entity has not documented or implemented any configuration change management process(es) (R1); ; OR

required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1); . OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration (1.2); OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration (1.3); OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from

			the existing baseline configuration (1.4.1); OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change (1.4.2 & 1.4.3); OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration (1.5.1); OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and

			production environments (1.5.2); OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6)

VSL Justifications for CIP-010-3, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	The addition of Part 1.6 does not lower the currentl level of compliance.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-010-3, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

Violation Risk Factor and Violation Severity Level Justifications

Project 2016-03 — Cyber Security — Supply Chain Risk Management

This document provides the drafting team's justification for assignment of violation risk factors (VRFs) and violation severity levels (VSLs) for each requirement in **Project 2016-03 — Cyber Security — Supply Chain Risk Management.** Each primary requirement is assigned a VRF and a set of one or more VSLs. These elements support the determination of an initial value range for the Base Penalty Amount regarding violations of requirements in FERC-approved Reliability Standards, as defined by the ERO Sanctions Guidelines. The Cyber Security Supply Chain Standard Drafting Team applied the following NERC criteria and FERC Guidelines when proposing VRFs and VSLs for the requirements under this project:

NERC Criteria for Violation Risk Factors

High Risk Requirement

A requirement that, if violated, could directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to bulk electric system instability, separation, or a cascading sequence of failures, or could place the bulk electric system at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to a normal condition.

Medium Risk Requirement

A requirement that, if violated, could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of a medium risk requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures; or, a requirement in a planning time frame that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly and adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. However, violation of a medium risk requirement is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to bulk electric system instability, separation, or cascading failures, nor to hinder restoration to a normal condition.

Lower Risk Requirement
A requirement that is administrative in nature and a requirement that, if violated, would not be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system; or, a requirement that is administrative in nature and a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to adversely affect the electrical state or capability of the bulk electric system, or the ability to effectively monitor, control, or restore the bulk electric system. A planning requirement that is administrative in nature.

FERC Guidelines for Violation Risk Factors

Guideline (1) – Consistency with the Conclusions of the Final Blackout Report

FERC seeks to ensure that VRFs assigned to Requirements of Reliability Standards in these identified areas appropriately reflect their historical critical impact on the reliability of the Bulk-Power System. In the VSL Order, FERC listed critical areas (from the Final Blackout Report) where violations could severely affect the reliability of the Bulk-Power System:

- Emergency operations
- Vegetation management
- Operator personnel training
- Protection systems and their coordination
- Operating tools and backup facilities
- Reactive power and voltage control
- System modeling and data exchange
- Communication protocol and facilities
- Requirements to determine equipment ratings
- Synchronized data recorders
- Clearer criteria for operationally critical facilities
- Appropriate use of transmission loading relief.

Guideline (2) – Consistency within a Reliability Standard
FERC expects a rational connection between the sub-Requirement VRF assignments and the main Requirement VRF assignment.

Guideline (3) – Consistency among Reliability Standards
FERC expects the assignment of VRFs corresponding to Requirements that address similar reliability goals in different Reliability Standards would be treated comparably.

Guideline (4) – Consistency with NERC's Definition of the Violation Risk Factor Level
Guideline (4) was developed to evaluate whether the assignment of a particular VRF level conforms to NERC's definition of that risk level.

Guideline (5) – Treatment of Requirements that Co-mingle More Than One Obligation
Where a single Requirement co-mingles a higher risk reliability objective and a lesser risk reliability objective, the VRF assignment for such Requirements must not be watered down to reflect the lower risk level associated with the less important objective of the Reliability Standard.

NERC Criteria for Violation Severity Levels

VSLs define the degree to which compliance with a requirement was not achieved. Each requirement must have at least one VSL. While it is preferable to have four VSLs for each requirement, some requirements do not have multiple "degrees" of noncompliant performance and may have only one, two, or three VSLs.

VSLs should be based on NERC's overarching criteria shown in the table below:

Lower VSL	Moderate VSL	High VSL	Severe VSL
The performance or product measured almost meets the full intent of the requirement.	The performance or product measured meets the majority of the intent of the requirement.	The performance or product measured does not meet the majority of the intent of the requirement, but does meet some of the intent.	The performance or product measured does not substantively meet the intent of the requirement.

FERC Order of Violation Severity Levels

The FERC VSL guidelines are presented below, followed by an analysis of whether the VSLs proposed for each requirement in the standard meet the FERC Guidelines for assessing VSLs:

Guideline (1) – Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance

Compare the VSLs to any prior levels of non-compliance and avoid significant changes that may encourage a lower level of compliance than was required when levels of non-compliance were used.

Guideline (2) – Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties

A violation of a "binary" type requirement must be a "Severe" VSL.

Do not use ambiguous terms such as "minor" and "significant" to describe noncompliant performance.

Guideline (3) – Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement

VSLs should not expand on what is required in the requirement.

Guideline (4) – Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations

Unless otherwise stated in the requirement, each instance of non-compliance with a requirement is a separate violation. Section 4 of the Sanction Guidelines states that assessing penalties on a per violation per day basis is the "default" for penalty calculations.

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in an Operations Planning time horizon to develop one or more documented supply chain cyber security risk management plan(s). If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-013-01, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective, which is to ~~address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle~~develop one or more documented supply chain cyber security risk management plan(s). Since the requirement has only one objective, only one VRF was assigned.

VSLs for CIP-013-1, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the ~~elements~~ parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the ~~elements~~ parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology. The VSL is assigned for a single instance of failing to develop one or more documented supply chain cyber security risk management plan(s) that set forth the controls.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in Operations Planning time horizon that requires entities to implement its supply chain cybersecurity risk management plan(s) specified in Requirement R1. If violated, failing to implement this plan could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R2			
Lower	**Moderate**	**High**	**Severe**
~~N/A~~ The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~N/A~~ The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	~~N/A~~ The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) as specified in the requirement.

VSL Justifications for CIP-013-1, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R2 is not binary. ~~The VSL assignment for R2 is SEVERE which is consistent with binary criteria.~~ Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSL is based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the plan specified in the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.~~A single VSL of Severe is assigned.~~
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-013-1, R3	
Proposed VRF	**Medium**
NERC VRF Discussion	R3 is a requirement in Operations Planning time horizon that requires the Responsible Entity to periodically review and obtain CIP Senior Manager or delegate approval of supply chain cyber security risk management plans. The reliability objective is to ensure plans remain up to date and address current and emerging supply chain-related cyber security concerns and vulnerabilities. If the requirement is violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a new requirement addressing specific reliability goals.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R3 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-013-1, R3			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within 18 calendar months of the previous review as specified in the Requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	There is no prior compliance obligation related to the subject of this standard.
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment is for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-013-1, R3	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of the review requirement by some number of months less than 18 calendar months does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-005-6, R2	
Proposed VRF	**Medium**
NERC VRF Discussion	R2 is a requirement in an Operations Planning and Same Day Operations time horizon to implement one or more documented processes for controlling vendor remote access to high and medium impact BES Cyber Systems. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report** This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with the addition of two parts addressing specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R2 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation.

VSLs for CIP-005-6, R2			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity does not have documented processes for one or more of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for one of the applicable items for Requirement Parts 2.1 through 2.3.	The Responsible Entity did not implement processes for two of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have either: one or more method(s) for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4); or one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5)..	The Responsible Entity did not implement processes for three of the applicable items for Requirement Parts 2.1 through 2.3; OR The Responsible Entity did not have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) (2.4) and one or more methods to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access) (2.5).

VSL Justifications for CIP-005-6, R2	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering	The~~re is no prior compliance obligation related to the subject of this standard~~addition of Parts 2.4 and 2.5 does not lower the current level of compliance.

the Current Level of Compliance	
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R2 is not binary. Guideline 2b: The proposed VSLs do not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.

FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
NERC VRF Discussion	R1 is a requirement in Operations Planning time horizon that requires the Responsible Entity to implement one or more documented processes that include each of the applicable requirement parts for configuration change management. If violated, it could directly affect the electrical state or the capability of the bulk electric system, or the ability to effectively monitor and control the bulk electric system. However, violation of the requirement is unlikely to lead to bulk electric system instability, separation, or cascading failures.
FERC VRF G1 Discussion	**Guideline 1- Consistency w/ Blackout Report**

VRF Justifications for CIP-010-1, R1	
Proposed VRF	**Medium**
	This requirement does not address any of the critical areas identified in the Final Blackout Report.
FERC VRF G2 Discussion	**Guideline 2- Consistency within a Reliability Standard** The requirement has no sub-requirements and is assigned a single VRF.
FERC VRF G3 Discussion	**Guideline 3- Consistency among Reliability Standards** This is a revised requirement with an additional part to address specific reliability goals. The VRF of Medium is consistent with the approved version of the standard.
FERC VRF G4 Discussion	**Guideline 4- Consistency with NERC Definitions of VRFs** A VRF of Medium is consistent with the NERC VRF definition as discussed above.
FERC VRF G5 Discussion	**Guideline 5- Treatment of Requirements that Co-mingle More than One Obligation** R1 contains only one objective and only one VRF was assigned. The requirement does not comingle more than one obligation

VSLs for CIP-010-3, R1			
Lower	**Moderate**	**High**	**Severe**
The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the	The Responsible Entity has not documented or implemented any configuration change management process(es) (R1); ; OR

required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	required baseline items listed in 1.1.1 through 1.1.5. (1.1) .	required baseline items listed in 1.1.1 through 1.1.5. (1.1) ~~;~~ OR ~~The Responsible Entity has~~ The Responsible Entity has a process as specified in Part 1.6 to verify the identity of the software source (1.6.1) but does not have a process as specified in Part 1.6 to verify the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6.2)~~.~~	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1); . OR The Responsible Entity does not have a process(es) that requires authorization and documentation of changes that deviate from the existing baseline configuration (1.2); OR The Responsible Entity does not have a process(es) to update baseline configurations within 30 calendar days of completing a change(s) that deviates from the existing baseline configuration (1.3); OR The Responsible Entity does not have a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from

			the existing baseline configuration (1.4.1); OR The Responsible Entity has a process(es) to determine required security controls in CIP-005 and CIP-007 that could be impacted by a change(s) that deviates from the existing baseline configuration but did not verify and document that the required controls were not adversely affected following the change (1.4.2 & 1.4.3); OR The Responsible Entity does not have a process for testing changes in an environment that models the baseline configuration prior to implementing a change that deviates from baseline configuration (1.5.1); OR The Responsible Entity does not have a process to document the test results and, if using a test environment, document the differences between the test and

			production environments (1.5.2); OR The Responsible Entity does not have a process as specified in Part 1.6 to verify the identity of the software source and the integrity of the software provided by the software source when the method to do so is available to the Responsible Entity from the software source. (1.6).

VSL Justifications for CIP-010-3, R1	
FERC VSL G1 Violation Severity Level Assignments Should Not Have the Unintended Consequence of Lowering the Current Level of Compliance	~~There~~ The addition of Part 1.6 does not lower the currentl level of compliance. ~~is no prior compliance obligation related to the subject of this standard.~~
FERC VSL G2 Violation Severity Level Assignments Should Ensure Uniformity and Consistency in the Determination of Penalties Guideline 2a: The Single Violation Severity Level Assignment Category for "Binary" Requirements Is Not Consistent Guideline 2b: Violation Severity Level Assignments that Contain Ambiguous Language	Guideline 2a: The VSL assignment for R1 is not binary. Guideline 2b: The proposed VSL does not use ambiguous terms, supporting uniformity and consistency in the determination of similar penalties for similar violations.
FERC VSL G3 Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement	The proposed VSL uses similar terminology to that used in the associated requirement, and is therefore consistent with the requirement.

VSL Justifications for CIP-010-3, R1	
FERC VSL G4 Violation Severity Level Assignment Should Be Based on A Single Violation, Not on A Cumulative Number of Violations	Proposed VSLs are based on a single violation and not a cumulative violation methodology.
FERC VSL G5 Requirements where a single lapse in protection can compromise computer network security, i.e., the 'weakest link' characteristic, should apply binary VSLs	An entity's violation of a single part of the requirement does not constitute a lapse in protection that compromises network security. Therefore a binary VSL is not warranted.
FERC VSL G6 VSLs for cyber security requirements containing interdependent tasks of documentation and implementation should account for their interdependence	There is no documentation and implementation interdependence within the requirement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise-Endorsed Implementation Guidance.
Endorsement for this implementation guidance is based on the language of "draft 2" of the CIP-013-1 Reliability Standard dated April 2017. Any changes to the standard prior to the final ballot will require a reevaluation of the implementation guidance for continued endorsement.

Cyber Security Supply Chain Risk Management Plans

Implementation Guidance for CIP-013-1

RELIABILITY | ACCOUNTABILITY




3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Introduction

On July 21, 2016, the Federal Energy Regulatory Commission (FERC) issued Order No. 829 directing the North American Electric Reliability Corporation (NERC) to develop a new or modified Reliability Standard that addresses cyber security supply chain risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations as follows:

> [The Commission directs] 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, [discussed in detail in the Order]: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Reliability Standard **CIP-013-1 – Cyber Security – Supply Chain Risk Management** addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the system life cycle for high and medium impact BES Cyber Systems[1].

This implementation guidance provides considerations for implementing the requirements in CIP-013-1 and examples of approaches that responsible entities could use to meet the requirements. The examples do not constitute the only approach to complying with CIP-013-1. Responsible Entities may choose alternative approaches that better fit their situation.

[1] Responsible Entities identify high and medium impact BES Cyber Systems according to the identification and categorization process required by CIP-002-5, or subsequent version of that standard.

Requirement R1

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:*

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;*

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).*

General Considerations for R1

The following are some general considerations for Responsible Entities as they implement Requirement R1:

First, in developing their supply chain cyber security risk management plan(s), Responsible entities should consider how to leverage the various components and phases of their processes (e.g. defined requirements, request for proposal, bid evaluation, external vendor assessment tools and data, third party certifications and audit reports, etc.) to help them meet the objective of Requirement R1 and give them flexibility to negotiate contracts with vendors to efficiently mitigate risks. Focusing solely on the negotiation of specific contract terms could have unintended consequences, including significant and unexpected cost increases for the product or service or vendors refusing to enter into contracts.

Additionally, a Responsible Entity may not have the ability to obtain each of its desired cyber security 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 terms and conditions ultimately negotiated by the parties and included in a contract. This variation in contract terms is 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.

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.

The focus of Requirement R1 is on the steps the Responsibility Entity takes to consider cyber security risks from vendor products or services during BES Cyber System planning and procurement. In the event the vendor is unwilling to engage in the negotiation process for cyber security controls, the Responsible Entity could explore other sources of supply or mitigating controls to reduce the risk to the BES cyber systems, as the Responsible Entity's circumstances allow.

In developing and implementing its supply chain cyber security risk management plan, a Responsible Entity may consider identifying and prioritizing security controls based on the cyber security 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 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 the Responsible Entities 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.

The objective of addressing the verification of software integrity and authenticity during the procurement phase of BES Cyber System(s) (Part 1.2.5) is to identify the capability of the vendor(s) to ensure that the software installed on BES Cyber System(s) is trustworthy. Part 1.2.5 is not an operational requirement for Responsible Entities to perform the verification; instead, Part 1.2.5 is aimed at identifying during the procurement phase the vendor's capability to provide software integrity and authenticity assurance and establish vendor performance based on the vendor's capability in order to implement CIP-010-3, Requirement R1, Part 1.6.

Implementation Guidance for R1

Responsible entities use various processes as they plan to procure BES Cyber Systems. Below are some examples of approaches to comply with this requirement:

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:*

- The Responsible Entity could establish one or more documents explaining the process by which the Responsible Entity will address supply chain cyber security risk management for high and medium impact BES Cyber Systems. To achieve the flexibility needed for supply chain cyber security risk management, Responsible Entities can use a "risk-based approach". 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. This flexibility is important to account for the varying "needs and characteristics of responsible entities and the diversity of BES Cyber System environments, technologies, and risk (FERC Order No. 829 P 44)."

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).*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when planning for the procurement of BES Cyber Systems to identify and assess cyber security risks to the Bulk Electric System from vendor products or services as specified in the requirement. Examples of processes, or outcomes of these processes, for complying with Part 1.1 are described below. A Responsible Entity could comply with Part 1.1 using either the first (team review) approach, or the second (risk assessment process) approach, a combination of the two approaches, or another approach determined by the Responsible Entity to comply with Part 1.1.

- A Responsible Entity can develop a process to form a team of subject matter experts from across the organization to participate in the BES Cyber System planning and acquisition process(es). The Responsible Entity should consider the relevant subject matter expertise necessary to meet the objective of Part 1.1 and include the appropriate representation of business operations, security architecture, information communications and technology, supply chain, compliance, and legal. Examples of factors that this team could consider in planning for the procurement of BES Cyber Systems as specified in Part 1.1 include:
  - Cyber security risk(s) to the BES that could be introduced by a vendor in new or planned modifications to BES Cyber Systems.
  - Vendor security processes and related procedures, including: system architecture, change control processes, remote access requirements, and security notification processes.
  - Periodic review processes that can be used with critical vendor(s) to review and assess any changes in vendor's security controls, product lifecycle management, supply chain, and roadmap to identify opportunities for continuous improvement.
  - Vendor use of third party (e.g., product/personnel certification processes) or independent review methods to verify product and/or service security practices.
  - Third-party security assessments or penetration testing provided by the vendors.
  - Vendor supply chain channels and plans to mitigate potential risks or disruptions.
  - Known system vulnerabilities; known threat techniques, tactics, and procedures; and related mitigation measures that could be introduced by vendor's information systems, components, or information system services.
  - Corporate governance and approval processes.
  - Methods to minimize network exposure, e.g., prevent internet accessibility, use of firewalls, and use of secure remote access techniques.
  - Methods to limit and/or control remote access from vendors to Responsible Entity's BES Cyber Systems.
  - Vendor's risk assessments and mitigation measures for cyber security during the planning and procurement process.
  - Mitigating controls that can be implemented by the Responsible Entity of the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.
- A Responsible Entity can develop a risk assessment process to identify and assess potential cyber security risks resulting from (i) procuring and installing vendor equipment and software and (ii) transitions from one vendor(s) to another vendor(s). This process could consider the following:
  - Potential risks based on the vendor's information systems, system components, and/or information system services / integrators. Examples of considerations include:

- Critical systems, components, or services that impact the operations or reliability of BES Cyber Systems.
- Product components that are not owned and managed by the vendor that may introduce additional risks, such as open source code or components from third party developers and manufacturers.

- Potential risks based on the vendor's risk management controls. Examples of vendor risk management controls to consider include[2]:
  - Personnel background and screening practices by vendors.
  - Training programs and assessments of vendor personnel on cyber security.
  - Formal vendor security programs which include their technical, organizational, and security management practices.
  - Vendor's physical and cyber security access controls to protect the facilities and product lifecycle.
  - Vendor's security engineering principles in (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security requirements into the system development lifecycle; (iv) delineating physical and logical security boundaries; (v) ensuring that system developers are training on how to build security software; (vi) tailoring security controls to meet organizational and operational needs; (vii) performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and (viii) reducing risk to acceptable levels, thus enabling informed risk management decisions. (NIST SP 800-53 SA-8 – Security Engineering Principles).
  - System Development Life Cycle program (SDLC) methodology from design through patch management to understand how cyber security is incorporated throughout the vendor's processes.
  - Vendor certifications and their alignment with recognized industry and regulatory controls.
  - Summary of any internal or independent cyber security testing performed on the vendor products to ensure secure and reliable operations.[3]
  - Vendor product roadmap describing vendor support of software patches, firmware updates, replacement parts and ongoing maintenance support.
  - Identify processes and controls for ongoing management of Responsible Entity and vendor's intellectual property ownership and responsibilities, if applicable. Examples include use of encryption algorithms for securing software code, data and information, designs, and proprietary processes while at rest or in transit.
- Based on risk assessment, identify mitigating controls that can be implemented by the Responsible Entity or the vendor. Examples include hardening the information system, minimizing the attack surface, ensuring ongoing support for system components, identification of alternate sources for critical components, etc.

[2] Tools such as the Standardized Information Gathering (SIG) Questionnaire from the Shared Assessments Program can aid in assessing vendor risk.

[3] For example, a Responsible Entity can request that the vendor provide a Standards for Attestation Engagements (SSAE) No. 18 SOC 2 audit report.

1.2. *One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:*

A Responsible Entity could document in its supply chain cyber security risk management plan one or more processes that it will use when procuring BES Cyber Systems to address Parts 1.2.1 through 1.2.6. The following are examples of processes, or outcomes of these processes, for complying with Part 1.2.

- Request cyber security terms relevant to applicable Parts 1.2.1 through 1.2.6 in the procurement process (request for proposal (RFP) or contract negotiation) for BES Cyber Systems to ensure that vendors understand the cyber security expectations for implementing proper security controls throughout the design, development, testing, manufacturing, delivery, installation, support, and disposition of the product lifecycle[4].
- During negotiations of procurement contracts or processes with vendors, the Responsible Entity can document the rationale, mitigating controls, or acceptance of deviations from the Responsible Entity's standard cyber security procurement language that is applicable to the vendor's system component, system integrators, or external service providers.

Examples of ways that a Responsible Entity could, through process(es) for procuring BES Cyber Systems required by Part 1.2, comply with Parts 1.2.1 through 1.2.6 are described below.

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;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification of any identified, threatened, attempted or successful breach of vendor's components, software or systems (*e.g.,* "security event") that have potential adverse impacts to the availability or reliability of BES Cyber Systems. Security event notifications to the Responsible Entity should be sent to designated point of contact as determined by the Responsible Entity and vendor. Examples of information to request that vendor's include in notifications to the Responsible Entity are(i) mitigating controls that the Responsible Entity can implement, if applicable (ii) availability of patch or corrective components, if applicable.

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;*

- A Responsible Entity and vendor can agree on service level agreements for response to cyber security incidents and commitment from vendor to collaborate with the Responsible Entity in implement mitigating controls and product corrections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that, in the event the vendor identifies a vulnerability that has resulted

[4] An example set of baseline supply chain cyber security procurement language for use by BES owners, operators, and vendors during the procurement process can be obtained from the "Cybersecurity Procurement Language for Energy Delivery Systems" developed by the Energy Sector Control Systems Working Group (ESCSWG).

in a cyber security incident related to the products or services provided to the Responsible Entity, the vendor should provide notification to Responsible Entity. The contract could specify that the vendor provide defined information regarding the products or services at risk and appropriate precautions available to minimize risks. Until the cyber security incident has been corrected, the vendor could be requested to perform analysis of information available or obtainable, provide an action plan, provide ongoing status reports, mitigating controls, and final resolution within reasonable periods as agreed on by vendor and Responsible Entity.

1.2.3. *1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;*

- In an RFP or during contract negotiations, request that the vendor include in the contract provisions an obligation for the vendor to provide notification to the Responsible Entity when vendor employee remote or onsite access should no longer be granted. This does not require the vendor to share sensitive information about vendor employees. Circumstances for no longer granting access to vendor employees include: (i) vendor determines that any of the persons permitted access is no longer required, (ii) persons permitted access are no longer qualified to maintain access, or (iii) vendor's employment of any of the persons permitted access is terminated for any reason. Request vendor cooperation in obtaining Responsible Entity notification within a negotiated period of time of such determination. The vendor and Responsible Entity should define alternative methods that will be implemented in order to continue ongoing operations or services as needed.
- If vendor utilizes third parties (or subcontractors) to perform services to Responsible Entity, require vendors to obtain Responsible Entity's prior approval and require third party's adherence to the requirements and access termination rights imposed on the vendor directly.

1.2.4. *Disclosure by vendors of known vulnerabilities;*

- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining access to summary documentation within a negotiated period of any identified security breaches involving the procured product or its supply chain that impact the availability or reliability of the Responsible Entity's BES Cyber System. Documentation should include a summary description of the breach, its potential security impact, its root cause, and recommended corrective actions involving the procured product.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor for cooperation in obtaining, within a negotiated time period after establishing appropriate confidentiality agreement, access to summary documentation of uncorrected security vulnerabilities in the procured product that have not been publicly disclosed. The summary documentation should include a description of each vulnerability and its potential impact, root cause, and recommended compensating security controls, mitigations, and/or procedural workarounds.
- During procurement, review with the vendor summary documentation of publicly disclosed vulnerabilities in the product being procured and the status of the vendor's disposition of those publicly disclosed vulnerabilities.

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*

- During procurement, request access to vendor documentation detailing the vendor patch management program and update process for all system components being procured (including third-party hardware, software, and firmware). This documentation should include the vendor's method or recommendation for how the integrity of the patch is validated by Responsible Entity. Ask vendors to describe the processes they use for delivering software and the methods that can be used to verify the integrity and authenticity of the software upon receipt, including systems with preinstalled software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide access to vendor documentation for the procured products (including third-party hardware, software, firmware, and services) regarding the release schedule and availability of updates and patches that should be considered or applied. Documentation should include instructions for securely applying, validating and testing the updates and patches.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within a reasonable period for duration of the product life cycle. Consideration regarding service level agreements for updates and patches to remediate critical vulnerabilities should be a shorter period than other updates. If updates cannot be made available by the vendor within a reasonable period, the vendor should be required to provide mitigations and/or workarounds.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to provide fingerprints or cipher hashes for all software so that the Responsible Entity can verify the values prior to installation on the BES Cyber System to verify the integrity of the software.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that when third-party software components are provided by the vendor, the vendors provide appropriate updates and patches to remediate newly discovered vulnerabilities or weaknesses of the third-party software components.

1.2.6. *Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).*

- During procurement, request vendors specify specific IP addresses, ports, and minimum privileges required to perform remote access services.
- Request vendors use individual user accounts that can be configured to limit access and permissions.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor to maintain their IT assets (hardware, software and firmware) connecting to Responsible Entity network with current updates to remediate security vulnerabilities or weaknesses identified by the original OEM or Responsible Entity.
- During procurement, request vendors document their processes for restricting connections from unauthorized personnel. Vendor personnel are not authorized to disclose or share account credentials, passwords or established connections.
- In an RFP or during contract negotiations, request that the vendor include in contract provisions a commitment from the vendor such that for vendor system-to-system connections that may limit the Responsible Entity's capability to authenticate the personnel connecting from the vendor's systems, the vendor will maintain complete and accurate books, user logs, access credential data, records, and other information applicable to connection access activities for a negotiated time period.

Requirement R2

R2. *Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.*

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.

General Considerations for R2

Implementation of the supply chain cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36). Contracts entering the Responsible Entity's procurement process (e.g. through Request for Proposals) on or after the effective date are within scope of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in the contract do not determine whether the contract is within scope of CIP-013-1.

Requirement R3

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.*

General Considerations for R3

In the Requirement R3 review, responsible entities should consider new risks and available mitigation measures, which could come from a variety of sources that include NERC, DHS, and other sources.

Implementation Guidance for R3

Responsible entities use various processes to address this requirement. Below are some examples of approaches to comply with this requirement:

- A team of subject matter experts from across the organization representing appropriate business operations, security architecture, information communications and technology, supply chain, compliance, legal, etc. reviews the supply chain cyber security risk management plan at least once every 15 calendar months to reassess for any changes needed. Sources of information for changes include, but are not limited to:
  - Requirements or guidelines from regulatory agencies
  - Industry best practices and guidance that improve supply chain cyber security risk management controls (e.g. NERC, DOE, DHS, ICS-CERT, Canadian Cyber Incident Response Center (CCIRC), and NIST).
  - Mitigating controls to address new and emerging supply chain-related cyber security concerns and vulnerabilities
  - Internal organizational continuous improvement feedback regarding identified deficiencies, opportunities for improvement, and lessons learned.
- The CIP Senior Manager, or approved delegate, reviews any changes to the supply chain cyber security risk management plan at least once every 15 calendar months. Reviews may be more frequent based on the timing and scope of changes to the supply chain cyber security risk management plan(s). Upon approval of changes to the supply chain cyber security risk management plan(s), the CIP Senior Manager or approved delegate should provide appropriate communications to the affected organizations or individuals. Additionally, communications or training material may be developed to ensure any organizational areas affected by revisions are informed.

References

- Utilities Technology Council (UTC) “Cyber Supply Chain Risk management for Utilities – Roadmap for Implementation”
- ISO/IEC 27036 – Information Security in Supplier Relationships
- NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations System and Services Acquisition SA-3, SA-8 and SA-22
- NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Energy Sector Control Systems Working Group (ESCSWG) - “Cybersecurity Procurement Language for Energy Delivery Systems”

Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified 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.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.* The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations". High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the

Order No. 829 Citation	Directive / Guidance	Resolution
		development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities.
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed/modified standard(s) must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve	The directive is addressed by Requirements R1, R2, and R3 of proposed CIP-013-1. Requirement R1 specifies that entities must develop, and Requirement R2 specifies that entities must implement, one or more documented supply chain cyber security risk

Order No. 829 Citation	Directive / Guidance	Resolution
	these four objectives but have the flexibility as to how to reach the objective (i.e., 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")).	management plan(s) for high and medium impact BES Cyber Systems that include one or more process(es) for mitigating cyber security risks to BES Cyber Systems. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle. **Proposed CIP-013-1 Requirement R1** **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: **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

Order No. 829 Citation	Directive / Guidance	Resolution
		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; **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). **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability Standard CIP-003-6, Requirement R1, the Reliability Standard should require 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. This periodic assessment should better ensure	The directive is addressed in proposed CIP-013-1 Requirement R3. **Proposed CIP-013-1 Requirement R3** **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

Order No. 829 Citation	Directive / Guidance	Resolution
	that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	The directive is addressed in proposed CIP-013-1 Requirement R3 (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement R3:** Entities perform periodic assessment to keep plans up-to-date and, addressing current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC) *Implementation Guidance* developed by the drafting team and submitted for ERO endorsement includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and CIP-010-3 Requirements R1 Part 1.6. The 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. **Proposed CIP-010-3 Requirement R1** **R1.** Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*.

Order No. 829 Citation	Directive / Guidance	Resolution
		1.6. Prior to 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.
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5. The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. The objective of Requirement R2 Part 2.5 is for entities to have the ability to disable active remote access sessions in the event of a system breach. **Proposed CIP-005-6 Requirement R2** **R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically

Order No. 829 Citation	Directive / Guidance	Resolution
		feasible, in CIP-005-6 Table R2 –Remote Access Management.: **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).
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by CIP-005-6 Requirement R2 Part 2.5 (above).
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address 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. 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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).
Objective 4: Vendor Risk Management and Procurement Controls		
P 59	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. Specifically, NERC must address controls for	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).

Order No. 829 Citation	Directive / Guidance	Resolution
	the following topics: (1) vendor security event notification processes; (2) vendor personnel termination 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. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	

Order No. 829 Citation	Directive / Guidance	Resolution
P 43	[the Commission directs] that NERC, pursuant to section 215(d)(5) of the FPA, develop a forward-looking, objective-driven new or modified 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.	Proposed CIP-013-1 addresses the directive. The purpose of the proposed standard is: *To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.* The SDT believes prioritizing high and medium impact BES Cyber Systems in the supply chain cyber security risk management standards is an appropriate approach to meeting the directives in FERC Order No. 829 and focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed standards address directives requiring plans, processes, and controls for supply chain cyber security risk management for "industrial control system hardware, software, and services associated with bulk electric system operations". High and medium impact BES Cyber Systems, as categorized in CIP-002-5, generally describe assets that are critical to interconnected operations including transmission operations, reliability coordination, and balancing functions. The proposed requirements prioritize these cyber systems by specifying mandatory requirements, while entities retain flexibility for determining appropriate steps for addressing supply chain cyber security risks for low impact BES Cyber Systems. The approach provides an opportunity for industry to take measured steps to addressing complex supply chain cyber security risks using an established prioritization mechanism. The reliability benefit of a measured and prioritized approach is that it is more manageable for responsible entities to focus the

Order No. 829 Citation	Directive / Guidance	Resolution
		development of their plans, processes, and controls on the smaller subset of cyber assets that includes the most significant cyber assets. Additionally, the SDT anticipates that the proposed standards may provide some risk mitigation for low impact BES Cyber Systems even though the requirements do not specifically apply to low impact BES Cyber Systems. One way that reliability benefits may be extended to low-impact BES Cyber Systems through the approval of CIP-013-1 is by responsible entities that own all three classifications of cyber assets (high, medium, and low). These entities may use some or all of the processes in their cyber security risk management plans that meet the CIP-013-1 requirements to plan and procure cyber assets that are used in low impact BES Cyber Systems. Another potential way that the reliability benefits may be extended to low impact BES Cyber Systems is through vendor adoption of CIP-013-1 related security controls that the vendor voluntarily includes in low impact BES Cyber System contracts with responsible entities. ~~CIP-013-1 is applicable to high and medium impact BES Cyber Systems. The proposed applicability appropriately focuses industry resources on supply chain cyber security risk management for industrial control system hardware, software, and computing and networking services associated with BES operations.~~
P 44	[the Commission directs] NERC to submit the new or modified Reliability Standard within one year of the effective date of this Final Rule. NERC should submit an informational filing [by December 26, 2016] with a plan to address the Commission's directive.	The proposed/modified standard(s) must be filed by September 27, 2017. NERC filed its plan to address the directive on December 15, 2016.
P 45	The plan required by the new or modified Reliability Standard developed by NERC should address, at a minimum, the following	The directive is addressed by Requirements R1, R2, and R3 of proposed CIP-013-1.

Order No. 829 Citation	Directive / Guidance	Resolution
	four specific security objectives in the context of addressing supply chain management risks: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls. Responsible entities should be required to achieve these four objectives but have the flexibility as to how to reach the objective (i.e., 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")).	Requirement R1 specifies that entities must develop, and Requirement R2 specifies that entities must implement, one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems that include one or more process(es) for mitigating cyber security risks to BES Cyber Systems. The plans address the four objectives from Order No. 829 (P 45) during the planning, acquisition, and deployment phases of the system life cycle. **Proposed CIP-013-1 Requirement R1** **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: **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

Order No. 829 Citation	Directive / Guidance	Resolution
		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; **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). **Proposed CIP-013-1 Requirement R2** **R2.** Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.
P 46	The new or modified Reliability Standard should also require a periodic reassessment of the utility's selected controls. Consistent with or similar to the requirement in Reliability	The directive is addressed in proposed CIP-013-1 Requirement R3. **Proposed CIP-013-1 Requirement R3**

Order No. 829 Citation	Directive / Guidance	Resolution
	Standard CIP-003-6, Requirement R1, the Reliability Standard should require 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. This periodic assessment should better ensure that the required plan remains up-to-date, addressing current and emerging supply chain-related concerns and vulnerabilities.	**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
p 47	Also, consistent with this reliance on an objectives-based approach, and as part of this periodic review and approval, the responsible entity's CIP Senior Manager should consider any guidance issued by NERC, the U.S. Department of Homeland Security (DHS) or other relevant authorities for the planning, procurement, and operation of industrial control systems and supporting information systems equipment since the prior approval, and identify any changes made to address the recent guidance.	The directive is addressed in proposed CIP-013-1 Requirement R3 (shown above) and supporting guidance. **Proposed CIP-013-1 Rationale for Requirement R3:** Entities perform periodic assessment to keep -plans up-to-date and, addressing current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by: •NERC or the E-ISAC •ICS-CERT •Canadian Cyber Incident Response Centre (CCIRC) *Implementation Guidance* developed by the drafting team and submitted for ERO endorsement includes example controls.
Objective 1: Software Integrity and Authenticity		
P 48	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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2.5 (discussed above) and CIP-010-3 Requirements R1 Part 1.6. The 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. **Proposed CIP-010-3 Requirement R1**

Order No. 829 Citation	Directive / Guidance	Resolution
		R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-010-3 Table R1 – Configuration Change Management*. **1.6.** ~~For a~~Prior to 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.
Objective 2: Vendor Remote Access to BES Cyber Systems		
P 51	The new or modified Reliability Standard must address responsible entities' logging and controlling all third-party (i.e., vendor) initiated remote access sessions. This objective covers both user-initiated and machine-to-machine vendor remote access.	The directive is addressed by proposed CIP-005-6 Requirement R2 Parts 2.4 and 2.5. The objective is to mitigate potential risks of a compromise at a vendor during an active remote access session with a Responsible Entity from impacting the BES. The objective of Requirement R2 Part 2.4 is for entities to have visibility of active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access) that are taking place on their system. The obligation in Part 2.4 requires entities to have a method to determine active vendor remote access sessions. The objective of Requirement R2 Part 2.5 is for entities to have the ability to ~~rapidly~~ disable active remote access sessions in the event of a system breach.

Order No. 829 Citation	Directive / Guidance	Resolution
		Proposed CIP-005-6 Requirement R2 **R2.** Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-6 Table R2 –Remote Access Management.: **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).
P 52	In addition, controls adopted under this objective should give responsible entities the ability to rapidly disable remote access sessions in the event of a system breach.	The directive is addressed by CIP-005-6 Requirement R2 Part 2.5 (above).
Objective 3: Information System Planning and Procurement		
P 56	As part of this objective, the new or modified Reliability Standard must address 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. 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.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.1 (shown above).
Objective 4: Vendor Risk Management and Procurement Controls		

Order No. 829 Citation	Directive / Guidance	Resolution
P 59	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. Specifically, NERC must address controls for the following topics: (1) vendor security event notification processes; (2) vendor personnel termination 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. NERC should also consider provisions to help responsible entities obtain necessary information from their vendors to minimize potential disruptions from vendor-related security events.	The directive is addressed in proposed CIP-013-1 Requirement R1 Part 1.2 (shown above).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2016-03 Cyber Security Supply Chain Risk Management CIP-005-6, CIP-010-3, and CIP-013-1

Final Ballots Open through July 20, 2017

Now Available

Final ballots are open through **8 p.m. Eastern, Thursday, July 20, 2017** for the following standards:

1. CIP-005-6 - Cyber Security – Electronic Security Perimeter(s);
2. CIP-010-3 - Cyber Security – Configuration Change Management and Vulnerability Assessments; and
3. CIP-013-1 - Cyber Security – Supply Chain Risk Management.

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pools associated with this project can log in and submit their votes here. If you experience any difficulties using the Standards Balloting & Commenting System (SBS), contact Nasheema Santos.

If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).

- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballots close. If approved, the standards will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, contact Senior Standards Developer, Mark Olson (via email) or at (404) 446-9760.

North American Electric Reliability Corporation
3353 Peachtree Rd, NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

BALLOT RESULTS

Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-005-6 FN 2 ST
Voting Start Date: 7/11/2017 9:51:02 AM
Voting End Date: 7/20/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 2
Total # Votes: 319
Total Ballot Pool: 391
Quorum: 81.59
Weighted Segment Value: 88.79

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	101	1	70	0.875	10	0.125	0	2	19
Segment: 2	7	0.6	6	0.6	0	0	0	0	1
Segment: 3	88	1	60	0.845	11	0.155	0	0	17
Segment: 4	24	1	16	0.8	4	0.2	0	1	3
Segment: 5	92	1	60	0.87	9	0.13	0	3	20
Segment: 6	62	1	47	0.87	7	0.13	0	0	8
Segment: 7	3	0.1	1	0.1	0	0	0	2	0
Segment: 8	4	0.1	1	0.1	0	0	0	0	3
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	9	0.7	7	0.7	0	0	0	1	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	391	6.6	269	5.86	41	0.74	0	9	72

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	N/A
1	AES - Dayton Power and Light Co.	Hertzel Shamash		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Mike Magruder	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Patricia Robertson		Affirmative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		None	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Brandon Ware		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	CPS Energy	Gladys DeLaO		Negative	N/A
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Affirmative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Negative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Affirmative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Affirmative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	VELCO -Vermont Electric Power Company, Inc.	Randy Buswell		Affirmative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	ISO New England, Inc.	Michael Puscas		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Aaron Austin		Negative	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		None	N/A
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Negative	N/A
3	Lincoln Electric System	Jason Fortik		Affirmative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		None	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Darl Shimko		Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Affirmative	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Santee Cooper	James Poston		Affirmative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	LaGen	Richard Comeaux		Negative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kasey Bohannon		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Affirmative	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		Negative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Dynegy Inc.	Dan Roethemeyer		Abstain	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Affirmative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	MGE Energy - Madison Gas and Electric Co.	Steven Schultz		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Negative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Affirmative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Affirmative	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Abstain	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons	Amy Casuscelli	Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Negative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Affirmative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	MGE Energy - Madison Gas and Electric Co.	Robert Thorson		None	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Shivaz Chopra		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Affirmative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara	Luiggi Beretta	Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Affirmative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Affirmative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southeastern Power Administration	Douglas Spencer		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Abstain	N/A
8	David Kiguel	David Kiguel		None	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Affirmative	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 391 of 391 entries

BALLOT RESULTS

Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-010-3 FN 2 ST
Voting Start Date: 7/11/2017 9:51:16 AM
Voting End Date: 7/20/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 2
Total # Votes: 318
Total Ballot Pool: 391
Quorum: 81.33
Weighted Segment Value: 81.4

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	101	1	65	0.823	14	0.177	0	2	20
Segment: 2	7	0.6	4	0.4	2	0.2	0	0	1
Segment: 3	88	1	55	0.775	16	0.225	0	0	17
Segment: 4	24	1	16	0.8	4	0.2	0	1	3
Segment: 5	92	1	55	0.797	14	0.203	0	3	20
Segment: 6	62	1	43	0.796	11	0.204	0	0	8
Segment: 7	3	0.1	1	0.1	0	0	0	2	0
Segment: 8	4	0.1	1	0.1	0	0	0	0	3
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	9	0.6	6	0.6	0	0	0	2	1

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	391	6.5	247	5.291	61	1.209	0	10	73

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Negative	N/A
1	AES - Dayton Power and Light Co.	Hertzel Shamash		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Mike Magruder	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Patricia Robertson		Negative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	N/A
1	Berkshire Hathaway Energy - MidAmerican Energy Co.	Terry Harbour		None	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	Cleco Corporation	John Lindsey	Louis Guidry	Negative	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Brandon Ware		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	Corn Belt Power Cooperative	larry brusseau		None	N/A
1	CPS Energy	Gladys DeLaO		Negative	N/A
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Negative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Negative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		None	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		Affirmative	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Affirmative	N/A
1	New York Power Authority	Salvatore Spagnolo		Affirmative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Negative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		None	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Negative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Affirmative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Affirmative	N/A
1	VELCO -Vermont Electric Power Company, Inc.	Randy Buswell		Affirmative	N/A
1	Westar Energy	Kevin Giles		Negative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Negative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	ISO New England, Inc.	Michael Puscas		Negative	N/A
2	Midcontinent ISO, Inc.	Terry Bllke		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	AEP	Aaron Austin		Negative	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		None	N/A
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	Cleco Corporation	Michelle Corley	Louis Guidry	Negative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Negative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A
3	Exelon	John Bee		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Negative	N/A
3	Lincoln Electric System	Jason Fortik		Negative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		None	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	MGE Energy - Madison Gas and Electric Co.	Darl Shimko		Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	N/A
3	New York Power Authority	David Rivera		Affirmative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		Affirmative	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	N/A
3	Puget Sound Energy, Inc.	Lynda Kupfer		Affirmative	N/A
3	Rutherford EMC	Tom Haire		None	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Santee Cooper	James Poston		Negative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A
3	Seattle City Light	Tuan Tran		Affirmative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	Tri-State G and T Association, Inc.	Janelle Marriott Gill		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Negative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Abstain	N/A
4	LaGen	Richard Comeaux		Negative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		None	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Affirmative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Negative	N/A
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kasey Bohannon		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		Affirmative	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		None	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Affirmative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	California Department of Water Resources	ASM Mostafa		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	Cleco Corporation	Stephanie Huffman	Louis Guidry	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		Negative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Dynegy Inc.	Dan Roethemeyer		Abstain	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Affirmative	N/A
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Entergy - Entergy Services, Inc.	Jaclyn Massey		None	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	MGE Energy - Madison Gas and Electric Co.	Steven Schultz		Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	N/A
5	New York Power Authority	Erick Barrios		Affirmative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Negative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Affirmative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Abstain	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Affirmative	N/A
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Negative	N/A
5	Xcel Energy, Inc.	David Lemmons	Amy Casuscelli	Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Negative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Negative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	MGE Energy - Madison Gas and Electric Co.	Robert Thorson		None	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	New York Power Authority	Shivaz Chopra		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		None	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Negative	N/A
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara	Luiggi Beretta	Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Affirmative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Negative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Southeastern Power Administration	Douglas Spencer		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Abstain	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Abstain	N/A
8	David Kiguel	David Kiguel		None	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Southwest Power Pool Regional Entity	Bob Reynolds		None	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 391 of 391 entries

BALLOT RESULTS

Ballot Name: 2016-03 Cyber Security Supply Chain Risk Management CIP-013-1 FN 3 ST
Voting Start Date: 7/11/2017 9:50:45 AM
Voting End Date: 7/20/2017 8:00:00 PM
Ballot Type: ST
Ballot Activity: FN
Ballot Series: 3
Total # Votes: 309
Total Ballot Pool: 373
Quorum: 82.84
Weighted Segment Value: 84.19

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Segment: 1	96	1	64	0.831	13	0.169	0	2	17
Segment: 2	7	0.6	6	0.6	0	0	0	0	1
Segment: 3	82	1	51	0.785	14	0.215	0	0	17
Segment: 4	24	1	16	0.727	6	0.273	0	0	2
Segment: 5	87	1	53	0.779	15	0.221	0	1	18
Segment: 6	61	1	45	0.818	10	0.182	0	0	6
Segment: 7	3	0.3	3	0.3	0	0	0	0	0
Segment: 8	4	0.1	1	0.1	0	0	0	0	3
Segment: 9	1	0.1	1	0.1	0	0	0	0	0
Segment: 10	8	0.6	6	0.6	0	0	0	2	0

Segment	Ballot Pool	Segment Weight	Affirmative Votes	Affirmative Fraction	Negative Votes w/ Comment	Negative Fraction w/ Comment	Negative Votes w/o Comment	Abstain	No Vote
Totals:	373	6.7	246	5.641	58	1.059	0	5	64

BALLOT POOL MEMBERS

Show All entries Search: Search

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	AEP - AEP Service Corporation	Dennis Sauriol		Affirmative	N/A
1	Allete - Minnesota Power, Inc.	Jamie Monette		Abstain	N/A
1	Ameren - Ameren Services	Eric Scott		Affirmative	N/A
1	American Transmission Company, LLC	Lauren Price		Affirmative	N/A
1	APS - Arizona Public Service Co.	Michelle Amarantos		Affirmative	N/A
1	Arizona Electric Power Cooperative, Inc.	John Shaver		None	N/A
1	Associated Electric Cooperative, Inc.	Mark Riley		Affirmative	N/A
1	Austin Energy	Thomas Standifur		None	N/A
1	Avista - Avista Corporation	Mike Magruder	Bradley Calbick	Affirmative	N/A
1	Balancing Authority of Northern California	Kevin Smith	Joe Tarantino	Affirmative	N/A
1	Basin Electric Power Cooperative	David Rudolph		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	BC Hydro and Power Authority	Patricia Robertson		Negative	N/A
1	Beaches Energy Services	Don Cuevas	Chris Gowder	Negative	N/A
1	Black Hills Corporation	Wes Wingen		Affirmative	N/A
1	Bonneville Power Administration	Kammy Rogers-Holliday		Affirmative	N/A
1	Brazos Electric Power Cooperative, Inc.	Tony Kroskey		None	N/A
1	CenterPoint Energy Houston Electric, LLC	John Brockhan		Affirmative	N/A
1	Central Electric Power Cooperative (Missouri)	Michael Bax		None	N/A
1	City Utilities of Springfield, Missouri	Michael Buyce		None	N/A
1	CMS Energy - Consumers Energy Company	James Anderson		Affirmative	N/A
1	Colorado Springs Utilities	Brandon Ware		Affirmative	N/A
1	Con Ed - Consolidated Edison Co. of New York	Daniel Grinkevich		Affirmative	N/A
1	CPS Energy	Gladys DeLaO		Affirmative	N/A
1	Dairyland Power Cooperative	Robert Roddy		None	N/A
1	Dominion - Dominion Virginia Power	Larry Nash		Affirmative	N/A
1	Duke Energy	Doug Hils		Affirmative	N/A
1	Edison International - Southern California Edison Company	Steven Mavis		Affirmative	N/A
1	El Paso Electric Company	Pablo Onate		Affirmative	N/A
1	Entergy - Entergy Services, Inc.	Oliver Burke		Affirmative	N/A
1	Eversource Energy	Quintin Lee		Affirmative	N/A
1	Exelon	Chris Scanlon		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	FirstEnergy - FirstEnergy Corporation	Karen Yoder		Affirmative	N/A
1	Florida Keys Electric Cooperative Assoc.	Dennis Minton		None	N/A
1	Georgia Transmission Corporation	Jason Snodgrass		Affirmative	N/A
1	Grand River Dam Authority	Stace Kegley		None	N/A
1	Great Plains Energy - Kansas City Power and Light Co.	James McBee	Douglas Webb	Affirmative	N/A
1	Great River Energy	Gordon Pietsch		Affirmative	N/A
1	Hydro One Networks, Inc.	Payam Farahbakhsh		Affirmative	N/A
1	Hydro-Qu?bec TransEnergie	Nicolas Turcotte		Affirmative	N/A
1	IDACORP - Idaho Power Company	Laura Nelson		Negative	N/A
1	Imperial Irrigation District	Jesus Sammy Alcaraz		Affirmative	N/A
1	International Transmission Company Holdings Corporation	Michael Moltane	Allie Gavin	Affirmative	N/A
1	JEA	Ted Hobson	Joe McClung	Affirmative	N/A
1	Lakeland Electric	Larry Watt		Negative	N/A
1	Lincoln Electric System	Danny Pudenz		Negative	N/A
1	Long Island Power Authority	Robert Ganley		Affirmative	N/A
1	Los Angeles Department of Water and Power	faranak sarbaz		Affirmative	N/A
1	Lower Colorado River Authority	Teresa Cantwell		Affirmative	N/A
1	M and A Electric Power Cooperative	William Price		None	N/A
1	Manitoba Hydro	Mike Smith		Affirmative	N/A
1	MEAG Power	David Weekley	Scott Miller	Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Memphis Light, Gas and Water Division	Allan Long		Affirmative	N/A
1	Minnkota Power Cooperative Inc.	Theresa Allard		Affirmative	N/A
1	Muscatine Power and Water	Andy Kurriger		None	N/A
1	N.W. Electric Power Cooperative, Inc.	Mark Ramsey		None	N/A
1	National Grid USA	Michael Jones		Affirmative	N/A
1	Nebraska Public Power District	Jamison Cawley		Negative	N/A
1	Network and Security Technologies	Nicholas Lauriat		Negative	N/A
1	New York Power Authority	Salvatore Spagnolo		Negative	N/A
1	NextEra Energy - Florida Power and Light Co.	Mike ONeil		Affirmative	N/A
1	Northeast Missouri Electric Power Cooperative	Kevin White		Affirmative	N/A
1	OGE Energy - Oklahoma Gas and Electric Co.	Terri Pyle		Affirmative	N/A
1	Ohio Valley Electric Corporation	Scott Cunningham		Affirmative	N/A
1	Omaha Public Power District	Doug Peterchuck		Affirmative	N/A
1	Oncor Electric Delivery	Lee Maurer	Linsey Ray	None	N/A
1	OTP - Otter Tail Power Company	Charles Wicklund		Affirmative	N/A
1	Peak Reliability	Scott Downey		Negative	N/A
1	Platte River Power Authority	Matt Thompson		Affirmative	N/A
1	PNM Resources - Public Service Company of New Mexico	Laurie Williams		None	N/A
1	Portland General Electric Co.	Scott Smith		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	PPL Electric Utilities Corporation	Brenda Truhe		Affirmative	N/A
1	PSEG - Public Service Electric and Gas Co.	Joseph Smith		Affirmative	N/A
1	Public Utility District No. 1 of Chelan County	Chad Bowman		Negative	N/A
1	Public Utility District No. 1 of Snohomish County	Long Duong		Affirmative	N/A
1	Public Utility District No. 2 of Grant County, Washington	Michiko Sell		None	N/A
1	Puget Sound Energy, Inc.	Theresa Rakowsky		Affirmative	N/A
1	Sacramento Municipal Utility District	Arthur Starkovich	Joe Tarantino	Affirmative	N/A
1	Salt River Project	Steven Cobb		Affirmative	N/A
1	Santee Cooper	Shawn Abrams		Negative	N/A
1	SaskPower	Wayne Guttormson		None	N/A
1	SCANA - South Carolina Electric and Gas Co.	Tom Hanzlik		Affirmative	N/A
1	Seattle City Light	Pawel Krupa		Negative	N/A
1	Seminole Electric Cooperative, Inc.	Mark Churilla	Dawn Hamdorf	None	N/A
1	Sempra - San Diego Gas and Electric	Martine Blair	Harold Sherrill	Affirmative	N/A
1	Sho-Me Power Electric Cooperative	Peter Dawson		Affirmative	N/A
1	Southern Company - Southern Company Services, Inc.	Katherine Prewitt		Affirmative	N/A
1	Southern Indiana Gas and Electric Co.	Steve Rawlinson		Affirmative	N/A
1	Sunflower Electric Power Corporation	Paul Mehlhaff		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
1	Tacoma Public Utilities (Tacoma, WA)	John Merrell		Abstain	N/A
1	Tallahassee Electric (City of Tallahassee, FL)	Scott Langston		None	N/A
1	Tennessee Valley Authority	Howell Scott		Affirmative	N/A
1	Tri-State G and T Association, Inc.	Tracy Sliman		Affirmative	N/A
1	U.S. Bureau of Reclamation	Richard Jackson		Negative	N/A
1	Westar Energy	Kevin Giles		Affirmative	N/A
1	Western Area Power Administration	sean erickson		Affirmative	N/A
1	Xcel Energy, Inc.	Dean Schiro		Affirmative	N/A
2	California ISO	Richard Vine		Affirmative	N/A
2	Electric Reliability Council of Texas, Inc.	Elizabeth Axson		Affirmative	N/A
2	Independent Electricity System Operator	Leonard Kula		None	N/A
2	ISO New England, Inc.	Michael Puscas		Affirmative	N/A
2	Midcontinent ISO, Inc.	Terry BIlke		Affirmative	N/A
2	PJM Interconnection, L.L.C.	Mark Holman		Affirmative	N/A
2	Southwest Power Pool, Inc. (RTO)	Charles Yeung		Affirmative	N/A
3	Ameren - Ameren Services	David Jendras		Affirmative	N/A
3	APS - Arizona Public Service Co.	Vivian Vo		Affirmative	N/A
3	Associated Electric Cooperative, Inc.	Todd Bennett		Affirmative	N/A
3	Austin Energy	W. Dwayne Preston		Affirmative	N/A
3	Avista - Avista Corporation	Scott Kinney		Affirmative	N/A
3	Basin Electric Power Cooperative	Jeremy Voll		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	BC Hydro and Power Authority	Hootan Jarollahi		Negative	N/A
3	Berkshire Hathaway Energy - MidAmerican Energy Co.	Annette Johnston	Darnez Gresham	Affirmative	N/A
3	Black Hills Corporation	Eric Egge	Maryanne Darling-Reich	Affirmative	N/A
3	Bonneville Power Administration	Rebecca Berdahl		Affirmative	N/A
3	Central Electric Power Cooperative (Missouri)	Adam Weber		None	N/A
3	City of Farmington	Linda Jacobson-Quinn		Affirmative	N/A
3	City of Leesburg	Chris Adkins	Chris Gowder	Negative	N/A
3	City of Vero Beach	Ginny Beigel	Chris Gowder	Negative	N/A
3	City Utilities of Springfield, Missouri	Scott Williams		None	N/A
3	Clark Public Utilities	Jack Stamper		Affirmative	N/A
3	CMS Energy - Consumers Energy Company	Karl Blaszkowski		Affirmative	N/A
3	Colorado Springs Utilities	Hillary Dobson		Affirmative	N/A
3	Con Ed - Consolidated Edison Co. of New York	Peter Yost		Affirmative	N/A
3	Cowlitz County PUD	Russell Noble		None	N/A
3	Dominion - Dominion Resources, Inc.	Connie Lowe		Affirmative	N/A
3	DTE Energy - Detroit Edison Company	Karie Barczak		None	N/A
3	Duke Energy	Lee Schuster		Affirmative	N/A
3	Edison International - Southern California Edison Company	Romel Aquino		Affirmative	N/A
3	El Paso Electric Company	Rhonda Bryant		Affirmative	N/A
3	Eversource Energy	Mark Kenny		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Exelon	John Bee		Affirmative	N/A
3	FirstEnergy - FirstEnergy Corporation	Aaron Ghodooshim		Affirmative	N/A
3	Florida Municipal Power Agency	Joe McKinney	Chris Gowder	Negative	N/A
3	Gainesville Regional Utilities	Ken Simmons	Chris Gowder	Negative	N/A
3	Georgia System Operations Corporation	Scott McGough		Affirmative	N/A
3	Great Plains Energy - Kansas City Power and Light Co.	Jessica Tucker	Douglas Webb	Affirmative	N/A
3	Great River Energy	Brian Glover		None	N/A
3	Hydro One Networks, Inc.	Paul Malozewski	Mike Beuthling	Affirmative	N/A
3	JEA	Garry Baker		None	N/A
3	KAMO Electric Cooperative	Ted Hilmes		Affirmative	N/A
3	Lakeland Electric	David Hadzima		Negative	N/A
3	Lincoln Electric System	Jason Fortik		Negative	N/A
3	Los Angeles Department of Water and Power	Mike Anctil		None	N/A
3	M and A Electric Power Cooperative	Stephen Pogue		None	N/A
3	Manitoba Hydro	Karim Abdel-Hadi		None	N/A
3	MEAG Power	Roger Brand	Scott Miller	Affirmative	N/A
3	Modesto Irrigation District	Jack Savage	Nick Braden	Affirmative	N/A
3	Muscatine Power and Water	Seth Shoemaker		Affirmative	N/A
3	National Grid USA	Brian Shanahan		Affirmative	N/A
3	Nebraska Public Power District	Tony Eddleman		Negative	N/A
3	New York Power Authority	David Rivera		Negative	N/A
3	NiSource - Northern Indiana Public Service Co.	Aimee Harris		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	North Carolina Electric Membership Corporation	doug white	Scott Brame	Affirmative	N/A
3	Northeast Missouri Electric Power Cooperative	Skyler Wiegmann		Affirmative	N/A
3	NRG - NRG Energy Power Marketing, Inc.	Rick Keetch		Negative	N/A
3	NW Electric Power Cooperative, Inc.	John Stickley		None	N/A
3	Ocala Utility Services	Randy Hahn		None	N/A
3	OGE Energy - Oklahoma Gas and Electric Co.	Donald Hargrove		Affirmative	N/A
3	Omaha Public Power District	Aaron Smith		Affirmative	N/A
3	Orlando Utilities Commission	Ballard Mutters		None	N/A
3	OTP - Otter Tail Power Company	Wendi Olson		Affirmative	N/A
3	Owensboro Municipal Utilities	Thomas Lyons		Affirmative	N/A
3	Pacific Gas and Electric Company	John Hagen		Affirmative	N/A
3	Platte River Power Authority	Jeff Landis		Affirmative	N/A
3	PNM Resources - Public Service Company of New Mexico	Lynn Goldstein		None	N/A
3	PPL - Louisville Gas and Electric Co.	Charles Freibert		Affirmative	N/A
3	PSEG - Public Service Electric and Gas Co.	Jeffrey Mueller		Affirmative	N/A
3	Public Utility District No. 1 of Chelan County	Joyce Gundry		Negative	N/A
3	Sacramento Municipal Utility District	Lori Folkman	Joe Tarantino	Affirmative	N/A
3	Salt River Project	Rudy Navarro		Affirmative	N/A
3	Santee Cooper	James Poston		Negative	N/A
3	SCANA - South Carolina Electric and Gas Co.	Clay Young		None	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
3	Seattle City Light	Tuan Tran		Negative	N/A
3	Seminole Electric Cooperative, Inc.	James Frauen		Negative	N/A
3	Sempra - San Diego Gas and Electric	Bridget Silvia	Jeff Johnson	Affirmative	N/A
3	Sho-Me Power Electric Cooperative	Jeff Neas		Affirmative	N/A
3	Snohomish County PUD No. 1	Mark Oens		Affirmative	N/A
3	Southern Company - Alabama Power Company	R. Scott Moore		Affirmative	N/A
3	Southern Indiana Gas and Electric Co.	Fred Frederick		Affirmative	N/A
3	Tacoma Public Utilities (Tacoma, WA)	Marc Donaldson		None	N/A
3	Tallahassee Electric (City of Tallahassee, FL)	John Williams		None	N/A
3	TECO - Tampa Electric Co.	Ronald Donahey		Affirmative	N/A
3	Tennessee Valley Authority	Ian Grant		Affirmative	N/A
3	WEC Energy Group, Inc.	Thomas Breene		Affirmative	N/A
3	Westar Energy	Bo Jones		Affirmative	N/A
3	Xcel Energy, Inc.	Michael Ibold		Affirmative	N/A
4	Alliant Energy Corporation Services, Inc.	Larry Heckert		Affirmative	N/A
4	Austin Energy	Esther Weekes		Affirmative	N/A
4	City of Clewiston	Lynne Mila	Chris Gowder	Negative	N/A
4	City Utilities of Springfield, Missouri	John Allen		None	N/A
4	CMS Energy - Consumers Energy Company	Beth Fields		Affirmative	N/A
4	FirstEnergy - FirstEnergy Corporation	Anthony Solic		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
4	Florida Municipal Power Agency	Carol Chinn	Chris Gowder	Negative	N/A
4	Georgia System Operations Corporation	Guy Andrews		Affirmative	N/A
4	Illinois Municipal Electric Agency	Mary Ann Todd		Affirmative	N/A
4	LaGen	Richard Comeaux		Negative	N/A
4	MGE Energy - Madison Gas and Electric Co.	Joseph DePoorter		Affirmative	N/A
4	Modesto Irrigation District	Spencer Tacke		None	N/A
4	National Rural Electric Cooperative Association	Barry Lawson		Affirmative	N/A
4	North Carolina Electric Membership Corporation	John Lemire	Scott Brame	Affirmative	N/A
4	Oklahoma Municipal Power Authority	Ashley Stringer		Affirmative	N/A
4	Public Utility District No. 1 of Snohomish County	John Martinsen		Affirmative	N/A
4	Public Utility District No. 2 of Grant County, Washington	Yvonne McMackin		Negative	N/A
4	Sacramento Municipal Utility District	Beth Tincher	Joe Tarantino	Affirmative	N/A
4	Seattle City Light	Hao Li		Negative	N/A
4	Seminole Electric Cooperative, Inc.	Michael Ward		Negative	N/A
4	South Mississippi Electric Power Association	Steve McElhaney		Affirmative	N/A
4	Tacoma Public Utilities (Tacoma, WA)	Hien Ho		Affirmative	N/A
4	Utility Services, Inc.	Brian Evans-Mongeon		Affirmative	N/A
4	WEC Energy Group, Inc.	Anthony Jankowski		Affirmative	N/A
5	AEP	Thomas Foltz		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Ameren - Ameren Missouri	Sam Dwyer		Affirmative	N/A
5	APS - Arizona Public Service Co.	Kasey Bohannon		Affirmative	N/A
5	Austin Energy	Jeanie Doty		Affirmative	N/A
5	Avista - Avista Corporation	Glen Farmer		None	N/A
5	Basin Electric Power Cooperative	Mike Kraft		Affirmative	N/A
5	BC Hydro and Power Authority	Helen Hamilton Harding		Negative	N/A
5	Berkshire Hathaway - NV Energy	Eric Schwarzrock		Affirmative	N/A
5	Black Hills Corporation	George Tatar		Affirmative	N/A
5	Boise-Kuna Irrigation District - Lucky Peak Power Plant Project	Mike Kukla		Negative	N/A
5	Bonneville Power Administration	Francis Halpin		Affirmative	N/A
5	Brazos Electric Power Cooperative, Inc.	Shari Heino		None	N/A
5	Calpine Corporation	Hamid Zakery		None	N/A
5	Choctaw Generation Limited Partnership, LLLP	Rob Watson		None	N/A
5	City Water, Light and Power of Springfield, IL	Steve Rose		None	N/A
5	CMS Energy - Consumers Energy Company	David Greyerbiehl		Affirmative	N/A
5	Colorado Springs Utilities	Jeff Icke		Affirmative	N/A
5	Con Ed - Consolidated Edison Co. of New York	Dermot Smyth		Affirmative	N/A
5	CPS Energy	Robert Stevens		Affirmative	N/A
5	Dairyland Power Cooperative	Tommy Drea		None	N/A
5	Dominion - Dominion Resources, Inc.	Lou Oberski		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	DTE Energy - Detroit Edison Company	Jeffrey DePriest		None	N/A
5	Duke Energy	Dale Goodwine		None	N/A
5	Edison International - Southern California Edison Company	Thomas Rafferty		Affirmative	N/A
5	EDP Renewables North America LLC	Heather Morgan		Negative	N/A
5	El Paso Electric Company	Victor Garzon		Affirmative	N/A
5	Eversource Energy	Timothy Reyher		Affirmative	N/A
5	Exelon	Ruth Miller		Affirmative	N/A
5	FirstEnergy - FirstEnergy Solutions	Robert Loy		Affirmative	N/A
5	Florida Municipal Power Agency	David Schumann	Chris Gowder	Negative	N/A
5	Great Plains Energy - Kansas City Power and Light Co.	Harold Wyble	Douglas Webb	Affirmative	N/A
5	Great River Energy	Preston Walsh		None	N/A
5	Herb Schrayshuen	Herb Schrayshuen		Affirmative	N/A
5	Hydro-Qu?bec Production	Normande Bouffard		Affirmative	N/A
5	JEA	John Babik		None	N/A
5	Kissimmee Utility Authority	Mike Blough		Negative	N/A
5	Lakeland Electric	Jim Howard		Negative	N/A
5	Lincoln Electric System	Kayleigh Wilkerson		Negative	N/A
5	Los Angeles Department of Water and Power	Kenneth Silver		None	N/A
5	Lower Colorado River Authority	Wesley Maurer		Affirmative	N/A
5	Luminant - Luminant Generation Company LLC	Alshare Hughes		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	Manitoba Hydro	Yuguang Xiao		Affirmative	N/A
5	Massachusetts Municipal Wholesale Electric Company	David Gordon		Affirmative	N/A
5	MEAG Power	Steven Grego	Scott Miller	Affirmative	N/A
5	Muscatine Power and Water	Neal Nelson		None	N/A
5	National Grid USA	Elizabeth Spivak		Affirmative	N/A
5	NB Power Corporation	Laura McLeod		None	N/A
5	Nebraska Public Power District	Don Schmit		Negative	N/A
5	New York Power Authority	Erick Barrios		Negative	N/A
5	NextEra Energy	Allen Schriver		Affirmative	N/A
5	NiSource - Northern Indiana Public Service Co.	Sarah Gasienica		Affirmative	N/A
5	North Carolina Electric Membership Corporation	Robert Beadle	Scott Brame	Affirmative	N/A
5	Northern California Power Agency	Marty Hostler		Affirmative	N/A
5	NRG - NRG Energy, Inc.	Patricia Lynch		Negative	N/A
5	OGE Energy - Oklahoma Gas and Electric Co.	John Rhea		None	N/A
5	Oglethorpe Power Corporation	Donna Johnson		None	N/A
5	Omaha Public Power District	Mahmood Safi		Affirmative	N/A
5	Ontario Power Generation Inc.	David Ramkalawan		Affirmative	N/A
5	Orlando Utilities Commission	Richard Kinas		Negative	N/A
5	OTP - Otter Tail Power Company	Cathy Fogale		Affirmative	N/A
5	Platte River Power Authority	Tyson Archie		Affirmative	N/A
5	Portland General Electric Co.	Ryan Olson		Affirmative	N/A
5	PPL - Louisville Gas and Electric Co.	Dan Wilson		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	PSEG - PSEG Fossil LLC	Tim Kucey		Affirmative	N/A
5	Public Utility District No. 1 of Chelan County	Haley Sousa		Negative	N/A
5	Public Utility District No. 1 of Snohomish County	Sam Nietfeld		Affirmative	N/A
5	Public Utility District No. 2 of Grant County, Washington	Alex Ybarra		None	N/A
5	Puget Sound Energy, Inc.	Eleanor Ewry		Affirmative	N/A
5	Sacramento Municipal Utility District	Susan Oto	Joe Tarantino	Affirmative	N/A
5	Salt River Project	Kevin Nielsen		Affirmative	N/A
5	Santee Cooper	Tommy Curtis		Negative	N/A
5	SCANA - South Carolina Electric and Gas Co.	Alyssa Hubbard		Affirmative	N/A
5	Seattle City Light	Mike Haynes		Negative	N/A
5	Seminole Electric Cooperative, Inc.	Brenda Atkins		None	N/A
5	Sempra - San Diego Gas and Electric	Jerome Gobby	Andrey Komissarov	Affirmative	N/A
5	Southern Company - Southern Company Generation	William D. Shultz		Affirmative	N/A
5	Southern Indiana Gas and Electric Co.	Scotty Brown	Rob Collins	Affirmative	N/A
5	SunPower	Bradley Collard		Affirmative	N/A
5	Tacoma Public Utilities (Tacoma, WA)	Chris Mattson		Abstain	N/A
5	Talen Generation, LLC	Donald Lock		None	N/A
5	TECO - Tampa Electric Co.	R James Rocha		Affirmative	N/A
5	Tennessee Valley Authority	M Lee Thomas		Affirmative	N/A
5	Tri-State G and T Association, Inc.	Mark Stein		Affirmative	N/A
5	U.S. Bureau of Reclamation	Wendy Center		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
5	WEC Energy Group, Inc.	Linda Horn		Affirmative	N/A
5	Westar Energy	Laura Cox		Affirmative	N/A
5	Xcel Energy, Inc.	David Lemmons	Amy Casuscelli	Affirmative	N/A
6	AEP - AEP Marketing	Dan Ewing		Affirmative	N/A
6	Ameren - Ameren Services	Robert Quinlivan		Affirmative	N/A
6	APS - Arizona Public Service Co.	Bobbi Welch		Affirmative	N/A
6	Associated Electric Cooperative, Inc.	Brian Ackermann		Affirmative	N/A
6	Austin Energy	Andrew Gallo		Affirmative	N/A
6	Basin Electric Power Cooperative	Paul Huettl		Affirmative	N/A
6	Berkshire Hathaway - PacifiCorp	Sandra Shaffer		Affirmative	N/A
6	Black Hills Corporation	Eric Scherr		Affirmative	N/A
6	Bonneville Power Administration	Andrew Meyers		Affirmative	N/A
6	Cleco Corporation	Robert Hirchak	Louis Guidry	Negative	N/A
6	Colorado Springs Utilities	Shannon Fair		Affirmative	N/A
6	Con Ed - Consolidated Edison Co. of New York	Robert Winston		Affirmative	N/A
6	Dominion - Dominion Resources, Inc.	Sean Bodkin		Affirmative	N/A
6	Duke Energy	Greg Cecil		Affirmative	N/A
6	Edison International - Southern California Edison Company	Kenya Streeter		Affirmative	N/A
6	El Paso Electric Company	Luis Rodriguez		None	N/A
6	Entergy	Julie Hall		Affirmative	N/A
6	Exelon	Becky Webb		Affirmative	N/A
6	FirstEnergy - FirstEnergy Solutions	Ann Ivanc		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	Florida Municipal Power Agency	Richard Montgomery	Chris Gowder	Negative	N/A
6	Florida Municipal Power Pool	Tom Reedy	Chris Gowder	Negative	N/A
6	Great Plains Energy - Kansas City Power and Light Co.	Chris Bridges	Douglas Webb	Affirmative	N/A
6	Great River Energy	Donna Stephenson	Michael Brytowski	Affirmative	N/A
6	Lakeland Electric	Paul Shipps		None	N/A
6	Lincoln Electric System	Eric Ruskamp		Negative	N/A
6	Los Angeles Department of Water and Power	Anton Vu		Affirmative	N/A
6	Lower Colorado River Authority	Michael Shaw		Affirmative	N/A
6	Luminant - Luminant Energy	Brenda Hampton		Affirmative	N/A
6	Manitoba Hydro	Blair Mukanik		Affirmative	N/A
6	Modesto Irrigation District	James McFall	Nick Braden	Affirmative	N/A
6	Muscatine Power and Water	Ryan Streck		Affirmative	N/A
6	New York Power Authority	Shivaz Chopra		Negative	N/A
6	NextEra Energy - Florida Power and Light Co.	Silvia Mitchell		Affirmative	N/A
6	NiSource - Northern Indiana Public Service Co.	Joe O'Brien		Affirmative	N/A
6	Northern California Power Agency	Dennis Sismaet		Affirmative	N/A
6	OGE Energy - Oklahoma Gas and Electric Co.	Jerry Nottnagel		Affirmative	N/A
6	Omaha Public Power District	Joel Robles		Affirmative	N/A
6	Platte River Power Authority	Sabrina Martz		Affirmative	N/A
6	Portland General Electric Co.	Daniel Mason		Affirmative	N/A
6	Powerex Corporation	Gordon Dobson-Mack		Negative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	PPL - Louisville Gas and Electric Co.	Linn Oelker		Affirmative	N/A
6	PSEG - PSEG Energy Resources and Trade LLC	Karla Jara		Affirmative	N/A
6	Public Utility District No. 1 of Chelan County	Janis Weddle		Negative	N/A
6	Public Utility District No. 2 of Grant County, Washington	LeRoy Patterson		Negative	N/A
6	Rayburn Country Electric Cooperative, Inc.	Greg Froehling		None	N/A
6	Sacramento Municipal Utility District	Jamie Cutlip	Joe Tarantino	Affirmative	N/A
6	Salt River Project	Bobby Olsen		Affirmative	N/A
6	Santee Cooper	Michael Brown		Negative	N/A
6	Seattle City Light	Charles Freeman		Affirmative	N/A
6	Seminole Electric Cooperative, Inc.	Trudy Novak		Negative	N/A
6	Snohomish County PUD No. 1	Franklin Lu		Affirmative	N/A
6	Southeastern Power Administration	Douglas Spencer		Affirmative	N/A
6	Southern Company - Southern Company Generation and Energy Marketing	Jennifer Sykes		Affirmative	N/A
6	Southern Indiana Gas and Electric Co.	Brad Lisembee		Affirmative	N/A
6	Tacoma Public Utilities (Tacoma, WA)	Rick Applegate		None	N/A
6	Talen Energy Marketing, LLC	Jennifer Hohenshilt		None	N/A
6	TECO - Tampa Electric Co.	Benjamin Smith		Affirmative	N/A
6	Tennessee Valley Authority	Marjorie Parsons		Affirmative	N/A

Segment	Organization	Voter	Designated Proxy	Ballot	NERC Memo
6	WEC Energy Group, Inc.	Scott Hoggatt		Affirmative	N/A
6	Westar Energy	Megan Wagner		None	N/A
6	Xcel Energy, Inc.	Carrie Dixon		Affirmative	N/A
7	Exxon Mobil	Jay Barnett		Affirmative	N/A
7	Luminant Mining Company LLC	Stewart Rake		Affirmative	N/A
7	Oxy - Occidental Chemical	Venona Greaff		Affirmative	N/A
8	David Kiguel	David Kiguel		None	N/A
8	Foundation for Resilient Societies	William Harris		None	N/A
8	Massachusetts Attorney General	Frederick Plett		None	N/A
8	Roger Zaklukiewicz	Roger Zaklukiewicz		Affirmative	N/A
9	Commonwealth of Massachusetts Department of Public Utilities	Donald Nelson		Affirmative	N/A
10	Florida Reliability Coordinating Council	Peter Heidrich		Affirmative	N/A
10	Midwest Reliability Organization	Russel Mountjoy		Affirmative	N/A
10	New York State Reliability Council	ALAN ADAMSON		Affirmative	N/A
10	Northeast Power Coordinating Council	Guy V. Zito		Affirmative	N/A
10	ReliabilityFirst	Anthony Jablonski		Abstain	N/A
10	SERC Reliability Corporation	David Greene		Affirmative	N/A
10	Texas Reliability Entity, Inc.	Rachel Coyne		Abstain	N/A
10	Western Electricity Coordinating Council	Steven Rueckert		Affirmative	N/A

Previous 1 Next

Showing 1 to 373 of 373 entries

Exhibit H

Standard Drafting Team Roster

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team Roster

Project 2016-03 Cyber Security Supply Chain Management

	Name	Entity
Chair	Corey Sellers	Southern Company
Vice-chair	JoAnn Murphy	PJM Interconnection, L.L.C.
Members	Christina Alston	Georgia Transmission Corp.
	James W. Chuber	Duke Energy
	Norm Dang	IESO of Ontario
	Chris Evans	Southwest Power Pool
	Brian Gatus	Southern California Edison Company
	David Bryan Gayle	Dominion Resources Services, Inc.
	Thruston J. Griffin	CPS Energy
	Skip Peeples	Salt River Project
	Jason Witt	East Kentucky Power Cooperative
PMOS Liaison	Brenda Hampton	Energy Future Holdings (Luminant)
NERC Staff	Mark Olson – Senior Standards Developer	North American Electric Reliability Corporation
	Laura Anderson – Standards Developer	North American Electric Reliability Corporation
	Shamai Elstein – Senior Counsel	North American Electric Reliability Corporation